



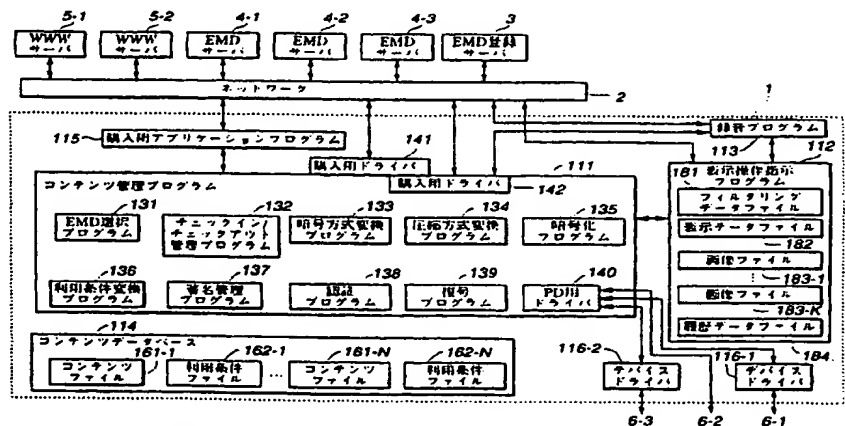
(51) 国際特許分類 G11B 20/10, G06F 12/14		A1	(11) 国際公開番号 WO00/39800
		(43) 国際公開日 2000年7月6日(06.07.00)	
(21) 国際出願番号 PCT/JP99/07302		(74) 代理人 小池 晃, 外(KOIKE, Akira et al.) 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo, (JP)	
(22) 国際出願日 1999年12月24日(24.12.99)			
(30) 優先権データ 特願平10/369414 1998年12月25日(25.12.98) JP 特願平11/39222 1999年2月17日(17.02.99) JP 特願平11/366086 1999年12月24日(24.12.99) JP			
(71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)		(81) 指定国 AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)	
(72) 発明者 ; および (75) 発明者 / 出願人 (米国についてののみ) 田辺 充(TANABE, Mitsuru)[JP/JP] 河上 達(KAWAKAMI, Itaru)[JP/JP] 石黒隆二(ISHIGURO, Ryuji)[JP/JP] 江面裕一(EZURA, Yuichi)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP)		添付公開書類 国際調査報告書 補正書	

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, AND PROGRAM STORAGE MEDIUM

(54) 発明の名称 情報処理装置及び方法、並びにプログラム格納媒体

(57) Abstract

A content database (114) contains identification information for identifying a content and time information on the time when the content is copied according to the identification information. An audio recording program (113) acquires the identification information on the content to be copied and copies the content according to the acquired identification information and time information stored in the content database (114). As a result, without greatly impairing the user's interests, a mass of copies are substantially inhibited.



5-1...WWW SERVER
5-2...WWW SERVER
4-1...EMD SERVER
4-2...EMD SERVER
4-3...EMD SERVER
3...END REGISTRATION SERVER
2...NETWORK
115...APPLICATION PROGRAM FOR PURCHASE
141...DRIVER FOR PURCHASE
142...DRIVER FOR PURCHASE
111...CONTENT MANAGING PROGRAM
131...EMD SELECTING PROGRAM
132...CHECK-IN/CHECK-OUT MANAGING PROGRAM
133...CIPHERING METHOD CONVERTING PROGRAM
134...COMPRESSION METHOD CONVERTING PROGRAM
135...CIPHERING PROGRAM
136...USE CONDITION CONVERTING PROGRAM
137...SIGNATURE MANAGING PROGRAM

138...AUTHENTICATION PROGRAM
139...DECIPHERING PROGRAM
140...DRIVER FOR PD
114...CONTENT DATABASE
161-1...CONTENT FILE
162-1...USE CONDITION FILE
161-N...CONTENT FILE
162-N...USE CONDITION FILE
116-2...DEVICE DRIVER
113...AUDIO RECORDING PROGRAM
112...DISPLAY INSTRUCTION PROGRAM
181...FILED DATA FILE
182...DISPLAY DATA FILE
183-1...IMAGE FILE
183-K...IMAGE FILE
184...HISTORY DATA FILE
116-1...DEVICE DRIVER

(57)要約

コンテンツデータベース 114 は、コンテンツを識別する識別情報と、識別情報に対応して、コンテンツが複製されたときの時刻情報を記憶する。録音プログラム 113 は、複製しようとするコンテンツの識別情報を取得して、取得された識別情報と、コンテンツデータベース 114 に記憶されている時刻情報に対応して、コンテンツを複製する。これにより、ユーザの利益を大きく損なうことなく、大量の複製を実質的に禁止する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	NZ	ニュージーランド		
CZ	チェッコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

明細書

情報処理装置及び方法、並びにプログラム格納媒体

技術分野

本発明は、情報処理装置及び方法、並びにプログラム格納媒体に関し、特に、例えば、コンテンツの複製を適切に制限することができるようにした情報処理装置及び方法、並びにプログラム格納媒体に関する。

背景技術

著作権が設定されているAVコンテンツ（例えば、音楽や画像）の複製を制限する方法として、SCMS (Serial Copy Management System)、CGMS (Copy Generation Management Sysytem)などが提案されている。

これらのシステムにおいては、図1に示すように、著作権が設定されたコンテンツA1（第1世代）を複製し、コンテンツA2（第2世代）を得ることは（記録することは）できるが、コンテンツA2（第2世代）自体をさらに複製して、コンテンツA3（第3世代）を得ることはできない。

発明の開示

しかしながら、この場合、図 1 に示すように、コンテンツ A 1 の複製を繰り返すことより、複数の第 2 世代のコンテンツ A 2 を得ることができ、コンテンツ A 1 の著作権が十分に保護されない課題があった。

そこで、コンテンツ A 1 を 1 度だけ複製することができるようにした方法として、UCS (Uni Copy System) が提案されているが、この場合、ユーザは、個人の使用の範囲においても、1 度だけしか複製することができず、ユーザに不利益を与える課題があった。

本発明はこのような状況に鑑みてなされたものであり、ユーザの利益を大きく損なうことなく、大量の複製を実質的に禁止することができるようにするものである。

本発明では、コンテンツを識別する識別情報と、識別情報に対応して、コンテンツが複製されたときの時刻情報が記憶され、複製しようとするコンテンツの識別情報が取得され、取得された識別情報と、記憶されている時刻情報に対応して、コンテンツが複製される。

すなわち、本発明に係る情報処理装置は、コンテンツを識別する識別情報と、識別情報に対応して、コンテンツが複製されたときの時刻情報を記憶する記憶手段と、複製しようとするコンテンツの識別情報を取得する取得手段と、取得手段により取得された識別情報と、記憶手段に記憶されている時刻情報に対応して、コンテンツを複製する複製手段とを含むことを特徴とする。

また、本発明に係る情報処理方法は、コンテンツを識別する識別情報と、識別情報に対応して、コンテンツが複製されたときの時刻情報を記憶する記憶ステップと、複製しようとするコンテンツの識別情報を取得する取得ステップと、取得ステップで取得された識別情報と、記憶ステップで記憶された時刻情報に対応して、コンテンツを複製する複製ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム格納媒体のプログラムは、コンテンツを識別する識別情報と、識別情報に対応して、コンテンツが複製されたときの時刻情報を記憶する記憶ステップと、複製しようとするコンテンツの識別情報を取得する取得ステップと、取得ステップで取得された識別情報と、記憶ステップで記憶された時刻情報に対応して、コンテンツを複製する複製ステップとを含むことを特徴とする。

図面の簡単な説明

図1は、SCMS及びCGMSを説明するための図である。

図2は、本発明に係る音声データ管理システムの一実施の形態を示す図である。

図3は、上記音声データ管理システムにおけるパーソナルコンピュータの構成を説明する図である。

図4は、上記音声データ管理システムにおけるポータブルデバイスの構成を説明する図である。

図5は、上記パーソナルコンピュータの機能の構成を説明するブ

ロック図である。

図 6 は、上記パーソナルコンピュータにおける録音プログラムがディスプレイに表示させるウィンドウの例を説明する図である。

図 7 は、上記パーソナルコンピュータにおいてコンパクトディスクから HDD にコピーする場合の処理を説明するフローチャートである。

図 8 は、図 7 に示したフローチャートにおけるステップ S 1 2 の期限データベースチェック処理を説明するフローチャートである。

図 9 は、期限データベースの例を示す図である。

図 1 0 は、ウォータマークを説明する図である。

図 1 1 は、曲データベースの例を示す図である。

図 1 2 A、図 1 2 B 及び 1 2 C は、HDD からポータブルデバイスへデータを移動する動作を説明するフローチャートである。

図 1 3 は、図 1 2 A に示したフローチャートにおけるステップ S 5 5 の選択曲の再生条件などのチェック処理を説明するフローチャートである。

図 1 4 は、ポータブルデバイス 6 が管理している再生条件を説明する図である。

図 1 5 は、図 1 2 A に示したフローチャートにおけるステップ S 5 8 のフォーマット変換処理の詳細を説明するフローチャートである。

図 1 6 A、図 1 6 B 及び図 1 6 C は、HDD 2 1 からポータブルデバイス 6 へデータをコピーする場合の動作を説明するフローチャートである。

図 1 7 は、ポータブルデバイスから HDD へデータを移動する場

合の動作を説明するフローチャートである。

図 1 8 は、ポータブルデバイスから HDD ヘデータをコピーする場合の動作を説明するフローチャートである。

図 1 9 は、EMD サーバから HDD ヘデータをコピーする場合の処理を説明するフローチャートである。

図 2 0 は、図 1 9 に示したフローチャートにおけるステップ S 2 0 4 の課金に関する処理の詳細を説明するフローチャートである。

図 2 1 は、課金ログを説明する図である。

図 2 2 A 及び図 2 2 B は、上記パーソナルコンピュータの I E C 6 0 9 5 8 端子から HDD ヘデータをコピーする場合の処理を説明するフローチャートである。

図 2 3 A 及び図 2 3 B は、HDD から I E C 6 0 9 5 8 端子にデータを出力する場合の動作を説明するフローチャートである。

図 2 4 は、図 2 3 A に示したフローチャートにおけるステップ S 2 7 5 の再生条件などのチェック処理を説明するフローチャートである。

図 2 5 A 及び図 2 5 B は、HDD からポータブルデバイス経由でデータを出力する場合の動作を説明するフローチャートである。

図 2 6 は、上記パーソナルコンピュータのアダプタに備えられた不揮発性メモリの機能を説明する図である。

図 2 7 は、上記アダプタの動作を説明するフローチャートである。

図 2 8 は、上記アダプタの内部の構成を示す図である。

図 2 9 A 及び図 2 9 B は、上記不揮発性メモリの内部の構成例を示す図である。

図 3 0 は、上記不揮発性メモリの内部の構成例を示す図である。

発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について、図面を参照しながら詳細に説明する。

図2は、本発明に係る音声データ管理システムの一実施の形態を示す図である。パーソナルコンピュータ1は、ローカルエリアネットワーク又はインターネットなどから構成されるネットワーク2に接続されている。パーソナルコンピュータ1は、EMD(Electrical Music Distribution)サーバ4-1乃至4-3から受信した、又は後述するCD(Compact Disc)から読み取った音楽のデータ(以下、コンテンツと称する)を、所定の圧縮の方式(例えば、ATRAC3(商標))に変換するとともにDES(Data Encryption Standard)などの暗号化方式で暗号化して記録する。

パーソナルコンピュータ1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に3台のポータブルデバイス(Portable Device(PDとも称する))6-1乃至6-3で利用できる、コピー(ポータブルデバイス6-1乃至6-3にコンテンツを記憶させても、パーソナルコンピュータ1が記録しているコンテンツは利用できる。ポータブルデバイス6-1乃至6-3にコンテンツを記憶させることができる回数は制限される場合がある。この場合、その回数は、増えることがない。)することができる、他のパーソナルコ

ンピュータに移動する（ポータブルデバイス 6-1 乃至 6-3 にコンテンツを記憶させた後、パーソナルコンピュータ 1 が記録しているコンテンツは使用できなくなる。）ことができるなどを示す。利用条件のデータの詳細は、後述する。

パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、又は再生条件など）とともに、USB(Universal Serial Bus)ケーブル 7-1 を介して、接続されているポータブルデバイス 6-1 に記憶させるとともに、ポータブルデバイス 6-1 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ 1 が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1 減らされる。チェックアウトできる回数が 0 のとき、対応するコンテンツは、チェックアウトすることができない。

パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、USBケーブル 7-2 を介して、接続されているポータブルデバイス 6-2 に記憶させるとともに、ポータブルデバイス 6-2 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、USBケーブル 7-3 を介して、接続されているポータブルデバイス 6-3 に記憶させるとともに、ポータブルデバイス 6-3 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

また、パーソナルコンピュータ 1 は、USB ケーブル 7-1 を介して、接続されているポータブルデバイス 6-1 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6-1 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ 1 が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1 増やされる。

パーソナルコンピュータ 1 は、USB ケーブル 7-2 を介して、接続されているポータブルデバイス 6-2 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6-2 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ 1 は、USB ケーブル 7-3 を介して、接続されているポータブルデバイス 6-3 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6-3 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

パーソナルコンピュータ 1 は、図示せぬ他のパーソナルコンピュータがポータブルデバイス 6-1 にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ 1 は、他のパーソナルコンピュータがポータブルデバイス 6-2 にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ 1 は、他のパーソナルコンピュータがポータブルデバイス 6-3 にチェックアウトしたコンテンツをチェックインできない。

EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4-1乃至4-3との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4-1乃至4-3に接続するためのプログラムをパーソナルコンピュータ1に送信する。

EMDサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ（例えば、曲名、又は再生制限など）とともに、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータとともに、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-3は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータとともに、パーソナルコンピュータ1にコンテンツを供給する。

EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一又は異なる圧縮の方式で圧縮されている。EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一又は異なる暗号化の方式で暗号化されている。

WWW(World Wide Web)サーバ5-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD（例えば、CDのアルバム名、又はCDの販売会社など）、及びCDから読み取ったコンテンツに対応するデータ（例え

ば、曲名、又は作曲者名など）をパーソナルコンピュータ 1 に供給する。WWWサーバ 5-2 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツを読み取った CD、及び CD から読み取ったコンテンツに対応するデータをパーソナルコンピュータ 1 に供給する。

ポータブルデバイス 6-1 は、パーソナルコンピュータ 1 から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、又は再生制限など）とともに記憶する。ポータブルデバイス 6-1 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス 6-1 は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス 6-1 は、対応するコンテンツの再生を停止する。

使用者は、コンテンツを記憶したポータブルデバイス 6-1 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス 6-2 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス 6-2 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフ

オンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6-2 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス 6-3 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス 6-3 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6-3 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

以下、ポータブルデバイス 6-1 乃至 6-3 を個々に区別する必要がないとき、単にポータブルデバイス 6 と称する。

図 3 は、パーソナルコンピュータ 1 の構成を説明する図である。CPU (Central Processing Unit) 11 は、各種アプリケーションプログラム（詳細については後述する）や、OS (Operating System) を実際に実行する。ROM (Read-only Memory) 12 は、一般的には、CPU 11 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 13 は、CPU 11 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらは CPU バスなどから構成されるホストバス 14 により相互に接続されている。

ホストバス 14 は、ブリッジ 15 を介して、PCI (Peripheral

Component Interconnect/Interface) バスなどの外部バス 16 に接続されている。

キーボード 18 は、CPU 11 に各種の指令を入力するとき、使用者により操作される。マウス 19 は、ディスプレイ 20 の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ 20 は、液晶表示装置又は CRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21 は、ハードディスクを駆動し、それらに CPU 11 によって実行するプログラムや情報を記録又は再生させる。

ドライブ 22 は、装着されている磁気ディスク 41、光ディスク 42 (CD を含む)、光磁気ディスク 43、又は半導体メモリ 44 に記録されているデータ又はプログラムを読み出して、そのデータ又はプログラムを、インターフェース 17、外部バス 16、ブリッジ 15、及びホストバス 14 を介して接続されている RAM 13 に供給する。

USB ポート 23-1 には、USB ケーブル 7-1 を介して、ポータブルデバイス 6-1 が接続される。USB ポート 23-1 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ (例えば、コンテンツ又はポータブルデバイス 6-1 のコマンドなどを含む) をポータブルデバイス 6-1 に出力する。

USB ポート 23-2 には、USB ケーブル 7-2 を介して、ポータブルデバイス 6-2 が接続される。USB ポート 23-2 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホスト

バス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-2 のコマンドなどを含む）をポータブルデバイス 6-2 に出力する。

USB ポート 23-3 には、USB ケーブル 7-3 を介して、ポータブルデバイス 6-3 が接続される。USB ポート 23-3 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-3 のコマンドなどを含む）をポータブルデバイス 6-3 に出力する。

IEC(International Electrotechnical Commission) 60958 端子を有する音声入出力インタフェース 24 は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ 45 は、音声入出力インタフェース 24 から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

これらのキーボード 18 乃至音声入出力インタフェース 24 は、インターフェース 17 に接続されており、インターフェース 17 は、外部バス 16、ブリッジ 15、及びホストバス 14 を介して CPU 11 に接続されている。

通信部 25 は、ネットワーク 2 が接続され、CPU 11、又は HDD 21 から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式の packets に格納して、ネットワーク 2 を介して、送信するとともに、ネットワーク 2 を介して、受信した packets に格納されているデータ（例えば、認証鍵、又は

コンテンツなど)をCPU 11、RAM 13、又はHDD 21に出力する。

半導体ICとして、一体的に形成され、パーソナルコンピュータ1に装着されるアダプタ26のCPU 32は、外部バス16、ブリッジ15、及びホストバス14を介してパーソナルコンピュータ1のCPU 11と共働し、各種の処理を実行する。RAM 33は、CPU 32が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ34は、パーソナルコンピュータ1の電源がオフされた後も保持する必要があるデータを記憶する。ROM 36には、パーソナルコンピュータ1から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC(Real Time Clock) 35は、計時動作を実行し、時刻情報を提供する。

通信部25及びアダプタ26は、外部バス16、ブリッジ15、及びホストバス14を介してCPU 11に接続されている。

以下、USBポート23-1乃至23-3を個々に区別する必要があるとき、単に、USBポート23と称する。以下、USBケーブル7-1乃至7-3を個々に区別する必要があるとき、単にUSBケーブル7と称する。

次に、ポータブルデバイス6の構成を図4を参照して説明する。電源回路52は、乾電池51から供給される電源電圧を所定の電圧の内部電力に変換して、CPU 53乃至表示部67に供給することにより、ポータブルデバイス6全体を駆動させる。

USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、

パーソナルコンピュータ 1 から転送されたコンテンツを、内部バス 58 を介して、CPU 53 に供給する。

コンテンツは、1 パケット当たり 64 バイトのデータから構成され、12 Mbit/sec の転送レートでパーソナルコンピュータ 1 から転送される。

ポータブルデバイス 6 に転送されるコンテンツは、ヘッダ及び音声データ（コンテンツの実体である、音声信号に対応したデータ）から構成され、ヘッダには、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデック ID、ファイル情報などが格納されているとともに、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限、及び再生回数カウンタなどが格納されている。音声データは、ATRAC3 などの符号化方式で符号化され、暗号化されている、所定の曲の音声信号に対応するデータである。

ヘッダサイズは、ヘッダのデータ長（例えば、33 バイトなど）を表し、ファイルサイズは、音声データのデータ長（例えば、33,636,138 バイトなど）を表す。

コンテンツ鍵は、暗号化されている音声データを復号するための鍵であり、パーソナルコンピュータ 1 とポータブルデバイス 6 との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ 1 からポータブルデバイス 6 に送信される。

ポータブルデバイス 6 が USB ケーブル 7 を介してパーソナルコンピュータ 1 の USB ポート 23 に接続されたとき、ポータブルデバイス 6 とパーソナルコンピュータ 1 とは、相互認証の処理を実行

する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス 6 の D S P 5 9 は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ 1 が生成するある値（チャレンジ）に対して、ポータブルデバイス 6 がパーソナルコンピュータ 1 と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ 1 が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス 6 が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ 1 は不正を検出できる。

コーデック I D は、音声データの符号化方式に対応した I D であり、例えば、コーデック I D ” 1 ” は、A T R A C 3 に対応し、コーデック I D ” 0 ” は、M P 3 (MPEG(Moving Picture Experts Group) Audio Layer-3) に対応する。

ファイル名は、コンテンツに対応するパーソナルコンピュータ 1 が記録しているコンテンツファイル（後述する）を A S C I I (American National Standard Code for Information Interchange) コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などを A S C I I コードに変換したデータである。

再生制限データは、コンテンツの再生が可能な期間（すなわち、

開始日時又は終了日時)又は回数制限(再生の回数の制限)が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、“1”が割り当てられ、再生が可能な期間が設定されているとき、“2”が割り当てられ、回数制限及び再生が可能な期間がいずれも設定されていないとき(いわゆる、買取りで購入されたとき)、“0”が割り当てられる。

開始日時及び終了日時は、再生制限データが“2”であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が“00040F”であり、終了日時が“00070F”であるとき、対応するコンテンツは、2000年4月15日から2000年7月15日まで、再生が可能である。

同様に、回数制限及び再生回数カウンタは、再生制限データが“1”又は“2”であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU53により更新される、コンテンツが再生された回数を示す。例えば、回数制限が“02”であるとき、そのコンテンツの再生可能な回数は2回であり、再生回数カウンタが“01”であるとき、そのコンテンツが再生された回数は1回である。

例えば、再生制限データが“2”であり、開始日時が“00040F”であり、終了日時が“00070F”であり、再生制限データが“2”であるとき、ポータブルデバイス6は、対応するコンテンツを、2000年4月15日から2000年7月15日までの期間において、1日2回ずつ繰り返し再生できる。

例えば、再生制限データが“1”であり、開始日時が“0000

00”であり、終了日時が”000000”であり、再生制限データが”0a”であり、再生回数カウンタが”05”であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が10回であり、再生された回数が5回である。

ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツとともにコンテンツの書き込み命令を受信した場合、ROM55からRAM54に読み出したメインプログラムを実行するCPU53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませる。

フラッシュメモリ61は、約64MByteの記憶容量を有し、コンテンツ（音声データ）を記憶する。また、フラッシュメモリ61には、所定の圧縮方式で圧縮されている音声データを伸張するための再生用コードが予め格納されている。

なお、フラッシュメモリ61は、ポータブルデバイス6に着脱可能とすることができる。

使用者による、図示せぬ再生／停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ62を介してCPU53に供給されると、CPU53は、フラッシュメモリコントローラ60に、フラッシュメモリ61から、再生用コードと音声データとを読み出させ、DSP59に転送させる。

DSP59は、フラッシュメモリ61から転送された再生用コードに基づいて音声データをCRC(Cyclic Redundancy Check)方式で誤り検出をした後、再生して、再生したデータ（図4中においてD1で示す）をディジタル／アナログ変換回路63に供給する。

DSP 59は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子59AからのマスタークロックMCLKを基に、音声データを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びにフレーム単位のLチャンネルクロックLCLK、及びRチャンネルクロックRCLKからなる動作クロックLRCLKをデジタルアナログ変換回路63に供給する。

DSP 59は、音声データを再生するとき、再生用コードに従って上述の動作クロックをデジタルアナログ変換回路63に供給して、音声データを再生しないとき、再生用コードに従って動作クロックの供給を停止して、デジタルアナログ変換回路63を停止させて、ポータブルデバイス6全体の消費電力量を低減する。

同様に、CPU 53及びUSBコントローラ57も、水晶でなる発振子53A又は57Aがそれぞれ外付けされ、発振子53A又は57Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

このように構成することで、ポータブルデバイス6は、CPU 53、DSP 59、USBコントローラ57等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

デジタルアナログ変換回路63は、再生した音声データをアナログの音声信号に変換して、これを増幅回路64に供給する。増幅回路64は、音声信号を増幅して、ヘッドフォンジャック65を介して、図示せぬヘッドフォンに音声信号を供給する。

このように、ポータブルデバイス 6 は、図示せぬ再生／停止ボタンが押圧操作されたとき、CPU 53 の制御に基づいてフラッシュメモリ 61 に記憶されている音声データを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、音声データの再生を停止する。

ポータブルデバイス 6 は、停止後に再度再生／停止ボタンが押圧操作されたとき、CPU 53 の制御に基づいて停止した位置から音声データの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス 6 は、自動的に電源をオフして消費電力を低減する。

因みに、ポータブルデバイス 6 は、電源がオフになった後に再生／停止ボタンが押圧操作されたとき、前回の停止した位置から音声データを再生せず、1 曲目から再生する。

また、ポータブルデバイス 6 の CPU 53 は、LCD コントローラ 68 を制御して、表示部 67 に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池 51 の残量等の情報を表示させる。

さらに、ポータブルデバイス 6 は、EEPROM 68 に、フラッシュメモリ 80 に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ 61 のブロック位置、及びその他種々のメモリ蓄積情報等のいわゆる FAT (File Allocation Table) を格納する。

因みに、本実施の形態においては、音声データは、64 K B y t

eを1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がF A Tに格納される。

フラッシュメモリ61にF A Tが格納される場合、例えば、1曲目のコンテンツがC P U 5 3の制御によりフラッシュメモリ61に書き込まれると、1曲目のコンテンツに対応するブロック位置がF A Tとしてフラッシュメモリ61に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ61に書き込まれると、2曲目のコンテンツに対応するブロック位置がF A Tとしてフラッシュメモリ61（1曲目と同一の領域）に書き込まれる。

このように、F A Tは、フラッシュメモリ61へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2重に書き込まれる。

F A Tがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書換えの回数に達してしまい、フラッシュメモリ61の書換えができなくなってしまう。

そこで、ポータブルデバイス6は、F A TをE E P R O M 6 8に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書換えの頻度を少なくしている。

書換えの回数の多いF A TをE E P R O M 6 8に記憶させることにより、F A Tをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、C P U 5 3は、E E P R O M 6 8にF A Tを追記するように書き込ませるので、E E P R

OM 6 8 の同一の領域の書換えの頻度を少なくして、EEPROM 6 8 が短時間で書換え不能になることを防止する。

ポータブルデバイス 6 は、USB ケーブル 7 を介してパーソナルコンピュータ 1 に接続されたとき（以下、これを USB 接続と称する）、USB コントローラ 5 7 から CPU 5 3 に供給される割り込み信号に基づき、USB 接続されたことを認識する。

ポータブルデバイス 6 は、USB 接続されたことを認識すると、パーソナルコンピュータ 1 から USB ケーブル 7 を介して規定電流値の外部電力の供給を受けるとともに、電源回路 5 2 を制御して、乾電池 5 1 からの電力の供給を停止させる。

CPU 5 3 は、USB 接続されたとき、DSP 5 9 の音声データの再生の処理を停止させる。これにより、CPU 5 3 は、パーソナルコンピュータ 1 から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

このように CPU 5 3 は、USB 接続されると、乾電池 5 1 から供給される電力からパーソナルコンピュータ 1 から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ 1 からの外部電力が使用され、電力単価の高い乾電池 5 1 の消費電力が低減され、かくして乾電池 5 1 の寿命を延ばすことができる。

なお、CPU 5 3 は、パーソナルコンピュータ 1 から USB ケーブル 7 を介して外部電力の供給を受けたとき、DSP 5 9 の再生処理を停止させることにより、DSP 5 9 からの輻射を低減させ、その結果としてパーソナルコンピュータ 1 を含むシステム全体の輻射を一段と低減させる。

図5は、CPU 11の所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を説明するブロック図である。コンテンツ管理プログラム111は、EMD選択プログラム131、チェックイン／チェックアウト管理プログラム132、暗号方式変換プログラム133、圧縮方式変換プログラム134、暗号化プログラム135、利用条件変換プログラム136、署名管理プログラム137、認証プログラム138、復号プログラム139、PD用ドライバ140、購入用ドライバ141、及び購入用ドライバ142などの複数のプログラムで構成されている。

コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム111を読み出しても、インストラクションを特定できないなど）ように構成されている。

EMD選択プログラム131は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム111には含まれず、後述するEMDの登録の処理において、ネットワーク2を介して、EMD登録サーバ3から受信される。EMD選択プログラム131は、EMDサーバ4-1乃至4-3のいずれかとの接続を選択して、購入用アプリケーション115、又は購入用ドライバ141若しくは142に、EMDサーバ4-1乃至4-3のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

チェックイン／チェックアウト管理プログラム132は、チェッ

クイン又はチェックアウトの設定、及びコンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に基づいて、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトするか、又はポータブルデバイス 6 - 1 乃至 6 - 3 に記憶されているコンテンツをチェックインする。

チェックイン/チェックアウト管理プログラム 1 3 2 は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータを更新する。

暗号方式変換プログラム 1 3 3 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの暗号化の方式、購入用ドライバ 1 4 1 が EMD サーバ 4 - 2 から受信したコンテンツの暗号化の方式、又は購入用ドライバ 1 4 2 が EMD サーバ 4 - 3 から受信したコンテンツの暗号化の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式に変換する。

また、暗号方式変換プログラム 1 3 3 は、ポータブルデバイス 6 - 1 又は 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 又は 6 - 3 が利用可能な暗号化方式に変換する。

圧縮方式変換プログラム 1 3 4 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの圧縮の方式、購入用ドライバ 1 4 1 が EMD

サーバ 4-2 から受信したコンテンツの圧縮の方式、又は購入用ドライバ 1 4 2 が EMD サーバ 4-3 から受信したコンテンツの圧縮の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1-1 乃至 1 6 1-N に格納されているコンテンツと同一の圧縮の方式に変換する。

圧縮方式変換プログラム 1 3 4 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1-1 乃至 1 6 1-N に格納されているコンテンツと同一の符号化の方式で符号化する。

また、圧縮方式変換プログラム 1 3 4 は、ポータブルデバイス 6-1 又は 6-3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6-1 又は 6-3 が利用可能な圧縮の方式に変換する。

暗号化プログラム 1 3 5 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1-1 乃至 1 6 1-N に格納されているコンテンツと同一の暗号化の方式で暗号化する。

利用条件変換プログラム 1 3 6 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4-1 から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用ドライバ 1 4 1 が EMD サーバ 4-2 から受信したコンテンツの利用条件を示すデータ、又は購入用ドライバ 1 4 2 が EMD サーバ 4-3 から受信したコンテンツの利用条件を示すデータ

を、コンテンツデータベース 1 1 4 が記録している利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件データと同一のフォーマットに変換する。

また、利用条件変換プログラム 1 3 6 は、ポータブルデバイス 6 - 1 又は 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス 6 - 1 又は 6 - 3 が利用可能な利用条件のデータに変換する。

署名管理プログラム 1 3 7 は、チェックイン又はチェックアウトの処理を実行する前に、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータに含まれている署名（後述する）を基に、利用条件のデータの改竄を検出する。署名管理プログラム 1 3 7 は、チェックイン又はチェックアウトの処理に伴う、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータを更新に対応して、利用条件のデータに含まれる署名を更新する。

認証プログラム 1 3 8 は、コンテンツ管理プログラム 1 1 1 と購入用アプリケーションプログラム 1 1 5 との相互認証の処理、及びコンテンツ管理プログラム 1 1 1 と購入用ドライバ 1 4 1 との相互認証の処理を実行する。また、認証プログラム 1 3 8 は、EMD サーバ 4 - 1 と購入用アプリケーションプログラム 1 1 5 との相互認証の処理、EMD サーバ 4 - 2 と購入用ドライバ 1 4 1 との相互認証の処理、及び EMD サーバ 4 - 3 と購入用ドライバ 1 4 2 との相互認証の処理で利用される認証鍵を記憶している。

認証プログラム 1 3 8 が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム 1 1 1 がパーソナルコンピュータ 1 にインストールされたとき、認証プログラム 1 3 8 に記憶されておらず、表示操作指示プログラム 1 1 2 により登録の処理が正常に実行されたとき、EMD 登録サーバ 3 から供給され、認証プログラム 1 3 8 に記憶される。

復号プログラム 1 3 9 は、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツをパーソナルコンピュータ 1 が再生するとき、コンテンツを復号する。

PD 用ドライバ 1 4 0 は、ポータブルデバイス 6 - 2 に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス 6 - 2 から所定のコンテンツをチェックインするとき、ポータブルデバイス 6 - 2 にコンテンツ又はポータブルデバイス 6 - 2 に所定の処理を実行させるコマンドを供給する。

PD 用ドライバ 1 4 0 は、ポータブルデバイス 6 - 1 に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス 6 - 1 から所定のコンテンツをチェックインするとき、デバイスドライバ 1 1 6 - 1 にコンテンツ、又はデバイスドライバ 1 1 6 - 1 に所定の処理を実行させるコマンドを供給する。

PD 用ドライバ 1 4 0 は、ポータブルデバイス 6 - 3 に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス 6 - 3 から所定のコンテンツをチェックインするとき、デバイスドライバ 1 1 6 - 2 にコンテンツ、又はデバイスドライバ 1 1 6 - 2 に所定の処理を実行させるコマンドを供給する。

購入用ドライバ141は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム111とともにインストールされ、EMD登録サーバ3からネットワーク2を介して供給され、又は所定のCDに記録されて供給される。購入用ドライバ141は、パーソナルコンピュータ1にインストールされたとき、コンテンツ管理プログラム111の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム111とデータを送受信する。

購入用ドライバ141は、ネットワーク2を介して、EMDサーバ4-2に所定のコンテンツの送信を要求するとともに、EMDサーバ4-2からコンテンツを受信する。また、購入用ドライバ141は、EMDサーバ4-2からコンテンツを受信するとき、課金の処理を実行する。

購入用ドライバ142は、コンテンツ管理プログラム111とともにインストールされるプログラムであり、ネットワーク2を介して、EMDサーバ4-3に所定のコンテンツの送信を要求するとともに、EMDサーバ4-3からコンテンツを受信する。また、購入用ドライバ142は、EMDサーバ4-3からコンテンツを受信するとき、課金の処理を実行する。

表示操作指示プログラム112は、フィルタリングデータファイル181、表示データファイル182、画像ファイル183-1乃至183-K、又は履歴データファイル184を基に、ディスプレイ20に所定のウィンドウの画像を表示させ、キーボード18又はマウス19への操作を基に、コンテンツ管理プログラム111にチェックイン又はチェックアウトなどの処理の実行を指示する。

フィルタリングデータファイル181は、コンテンツデータベ-

ス 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、H D D 2 1 に記録されている。

表示データファイル 1 8 2 は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツに対応するデータを格納して、H D D 2 1 に記録されている。

画像ファイル 1 8 3 - 1 乃至 1 8 3 - K は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に対応する画像、又は後述するパッケージに対応する画像を格納して、H D D 2 1 に記録されている。

以下、画像ファイル 1 8 3 - 1 乃至 1 8 3 - K を個々に区別する必要がないとき、単に、画像ファイル 1 8 3 と称する。

履歴データファイル 1 8 4 は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、H D D 2 1 に記録されている。

表示操作指示プログラム 1 1 2 は、登録の処理のとき、ネットワーク 2 を介して、E M D 登録サーバ 3 に、予め記憶しているコンテンツ管理プログラム 1 1 1 の I D を送信するとともに、E M D 登録サーバ 3 から認証用鍵及び E M D 選択プログラム 1 3 1 を受信して、コンテンツ管理プログラム 1 1 1 に認証用鍵及び E M D 選択プログラム 1 3 1 を供給する。

録音プログラム 1 1 3 は、所定のウィンドウの画像を表示させて、

キーボード 18 又はマウス 19 への操作を基に、ドライブ 22 に装着された光ディスク 42 である CD からコンテンツの録音時間などのデータを読み出す。

録音プログラム 113 は、CD に記録されているコンテンツの録音時間などを基に、ネットワーク 2 を介して、WWW サーバ 5-1 又は 5-2 に CD に対応するデータ（例えば、アルバム名、又はアーティスト名など）又は CD に記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWW サーバ 5-1 又は 5-2 から CD に対応するデータ又は CD に記録されているコンテンツに対応するデータを受信する。

録音プログラム 113 は、受信した CD に対応するデータ又は CD に記録されているコンテンツに対応するデータを、表示操作指示プログラム 112 に供給する。

また、録音の指示が入力されたとき、録音プログラム 113 は、ドライブ 22 に装着された光ディスク 42 である CD からコンテンツを読み出して、コンテンツ管理プログラム 111 に出力する。

コンテンツデータベース 114 は、コンテンツ管理プログラム 111 から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル 161-1 乃至 161-N のいずれかに格納する（HDD 21 に記録する）。コンテンツデータベース 114 は、コンテンツファイル 161-1 乃至 161-N にそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル 161-1 乃至 161-N にそれぞれ対応する利用条件ファイル 162-1 乃至 162-N のいずれかに格納する（HDD 21 に記録する）。

コンテンツデータベース 114 は、コンテンツファイル 161-1 乃至 161-N 又は利用条件ファイル 162-1 乃至 162-N をレコードとして記録してもよい。

例えば、コンテンツファイル 161-1 に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 162-1 に格納されている。コンテンツファイル 161-N に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 162-N に格納されている。

なお、利用条件ファイル 162-1 乃至 162-N に記録されているデータは、後述する期限データベースに記録されているデータ、又は曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース 114 は、後述する期限データベース及び曲データベースを包含して、構成されている。

以下、コンテンツファイル 161-1 乃至 161-N を個々に区別する必要がないとき、単に、コンテンツファイル 161 と称する。以下、利用条件ファイル 162-1 乃至 162-N を個々に区別する必要がないとき、単に、利用条件ファイル 162 と称する。

購入用アプリケーションプログラム 115 は、EMD 登録サーバ 3 からネットワーク 2 を介して供給され、又は所定の CD に記録されて供給される。購入用アプリケーションプログラム 115 は、ネットワーク 2 を介して、EMD サーバ 4-1 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-1 からコンテンツを受信して、コンテンツ管理プログラム 111 に供給する。また、購入用アプリケーションプログラム 115 は、EMD サーバ 4-1 からコンテンツを受信するとき、課金の処理を実行する。

次に、表示データファイル 8 2 に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N との対応付けについて説明する。

コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N のいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

オリジナルパッケージは、1 以上のコンテンツが属し、EMD サーバ 4 - 1 乃至 4 - 3 におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚の CD に対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

マイセレクトパッケージは、使用者が任意に選択した 1 以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1 以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

フィルタリングパッケージには、フィルタリングデータファイル 1 8 1 に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMD サーバ 4 - 1 乃至 4 - 3 又は WWW サーバ 5 - 1 若しくは 5 - 2 などからネット

ワーク 2 を介して供給され、又は所定の C D に記録されて供給される。使用者は、フィルタリングデータファイル 1 8 1 に格納されているフィルタリングデータを編集することができる。

フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週の J - P O P (日本のポップス) ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ 1 は、今週の日本のポップス 1 位のコンテンツ乃至今週の日本のポップス 1 0 位のコンテンツを特定することができる。

フィルタリングデータファイル 1 8 1 は、例えば、過去 1 月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に”愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ 2 2 1 (コンテンツ用表示データ 2 2 1 に使用者が設定したデータを含む)、又は履歴データ 1 8 4 などと、フィルタリングデータとを対応させて選択される。

図 6 は、WWWサーバ 5 - 2 から C D の情報を受信したとき、録音プログラム 1 1 3 がディスプレイ 2 0 に表示させるウィンドウを説明する図である。WWWサーバ 5 - 2 から受信した C D の情報を基に、録音プログラム 1 1 3 は、フィールド 2 0 1 に、例えば、”アシンクロナイズド”などの C D のタイトルを表示する。WWWサーバ 5 - 2 から受信した C D の情報を基に、録音プログラム 1 1 3

は、フィールド 2 0 2 に、例えば、” クワイ ” などのアーティスト名を表示する。

WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログラム 1 1 3 は、フィールド 2 0 3 の曲名を表示する部分に、例えば、” ヒート ” , ” プラネット ” , ” ブラック ” , ” ソウル ” などの曲名を表示する。同様に、録音プログラム 1 1 3 は、フィールド 2 0 3 のアーティストを表示する部分に、例えば、” クワイ ” などのアーティスト名を表示する。

録音プログラム 1 1 3 が所定の CD の情報を受信した後、録音プログラム 1 1 3 は、HDD 2 1 の所定のディレクトリに CD の情報を格納する。

ボタン 2 0 4 などがクリックされて、CD の情報の取得の指示を受けたとき、録音プログラム 1 1 3 は、始めに、HDD 2 1 の所定のディレクトリを検索する。録音プログラム 1 1 3 は、そのディレクトリに CD の情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている CD の情報を利用するか否かを選択させる。

録音プログラム 1 1 3 が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン 2 0 6 がクリックされたとき、録音プログラム 1 1 3 は、ドライブ 2 2 に格納されている CD からコンテンツを読み出して、CD から読み出したコンテンツを CD の情報とともにコンテンツ管理プログラム 1 1 1 に供給する。コンテンツ管理プログラム 1 1 1 の圧縮方式変換プログラム 1 3 4 は、録音プログラム 1 1 3 から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム 1 3 5 は、圧縮されたコンテ

ンツを、暗号化する。また、利用条件変換プログラム 1 3 6 は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

コンテンツ管理プログラム 1 1 1 は、圧縮され、暗号化されたコンテンツを利用条件のデータとともに、コンテンツデータベース 1 1 4 に供給する。

コンテンツデータベース 1 1 4 は、コンテンツ管理プログラム 1 1 1 から受信したコンテンツに対応するコンテンツファイル 1 6 1 及び利用条件ファイル 1 6 2 を生成して、コンテンツファイル 1 6 1 にコンテンツを格納するとともに、利用条件ファイル 1 6 2 に利用条件のデータを格納する。

コンテンツ管理プログラム 1 1 1 は、コンテンツデータベース 1 1 4 にコンテンツ及びコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム 1 1 3 から受信した CD の情報及び利用条件のデータを表示操作指示プログラム 1 1 2 に供給する。

表示操作指示プログラム 1 1 2 は、録音の処理でコンテンツデータベース 1 1 4 に格納されたコンテンツに対応する利用条件のデータ及び CD の情報を基に、オリジナルパッケージ用表示データ 2 0 1 及びコンテンツ用表示データ 2 2 1 を生成する。

録音プログラム 1 1 3 が表示させるウィンドウには、更に、CD から読み出したコンテンツをコンテンツデータベース 1 1 4 に記録したとき、自動的に、CD から読み出したコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトさせるか否かの設定を行うボタン 2 0 5 が配置されている。

例えば、ボタン 2 0 5 がクリックされたとき、録音プログラム 1

13は、ポータブルデバイス6-1乃至6-3のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス6-1乃至6-3のいずれかを選択したとき、パーソナルコンピュータ1は、選択されたポータブルデバイス6-1乃至6-3のいずれかに、自動的に、CDから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ1は、CDからコンテンツを記録したとき、チェックアウトしない。

次に、図7のフローチャートを参照して、録音プログラム113を実行するCPU11による、ドライブ22に装着されたCDから再生した音楽データをHDD21に転送し、コピーする場合の処理について説明する。使用者がキーボード18又はマウス19を操作して、インタフェース17を介してCPU11に対してドライブ22に装着されたCD（図示せず）から再生された音楽データをHDD21に転送、コピーする指令を入力すると、CPU11は、ステップS11において、インタフェース17を介してディスプレイ20にコピーする曲を選択するためのGUI(Graphical User Interface)を表示させる。

具体的には、例えば、CPU11は、ドライブ22に装着されたCDのTOC(Table Of Contents)を読み込み、そのCDに含まれる曲の情報を得て、ディスプレイ20に表示させる。又は、CPU11は、CDに含まれている各曲毎のISRC(International Standard Recording Code)を読み出し、その曲の情報を得て、ディスプレイ20に表示させる。あるいはまた、CPU11は、ネットワ

ーク 2 を介して WWW サーバ 5 - 1 又は 5 - 2 にアクセスし、T O C を用いて、その C D の曲の情報を得て、対応する G U I をディスプレイ 2 0 に表示させる。使用者は、ディスプレイ 2 0 の G U I を利用してキーボード 1 8 又はマウス 1 9 を操作し、コピーする曲を選択する。

次に、ステップ S 1 2 において、C P U 1 1 は、H D D 2 1 に格納されている期限データベース（図 5 に示すコンテンツデータベース 1 1 4 の利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に対応する）をチェックする。この期限データベースチェック処理の詳細は、図 8 のフローチャートに示されている。

ステップ S 3 1 において C P U 1 1 は、アダプタ 2 6 の C P U 3 2 と共働して、期限データベース全体のハッシュ値を計算し、ステップ S 3 2 において、その計算された値と、前回保存しておいたハッシュ値と比較する。

なお、期限データベースにデータが何ら記録されていないとき、C P U 1 1 は、ハッシュ値を計算しない。

すなわち、H D D 2 1 には、期限データベースが形成されており、この期限データベースには、図 9 に示すように、H D D 2 1 に記録されている音楽データ（コンテンツ）を管理する管理情報として、過去に記録されたことのある曲の I S R C とコピー日時が対応して記憶されている。この例においては、アイテム 1 乃至アイテム 3 の 3 つのアイテムについて、それぞれの I S R C とコピー日時が記憶されている。この期限データベースに記録されている全ての曲の I S R C とコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップ S 3 8 において、アダプタ 2 6 の C

P U 3 2 により計算され、不揮発性メモリ 3 4 に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、S H A (Secure Hash Algorithm) , M D (Message Digest) 5 などがある。C P U 1 1 は、ステップ S 3 1 において、C P U 3 2 が実行したのと同様にハッシュ値を計算する。そして、ステップ S 3 2 において、C P U 1 1 は、C P U 3 2 に、不揮発性メモリ 3 4 に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップ S 3 1 で、いま自分自身が計算したハッシュ値とを比較する。

ステップ S 3 3 において、C P U 1 1 は、ステップ S 3 1 でいま計算したハッシュ値と、不揮発性メモリ 3 4 に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、C P U 1 1 は、ステップ S 3 4 において、例えば、「期限データベースが改竄されたので、コピーができません」といったメッセージを発生し、インタフェース 1 7 を介してディスプレイ 2 0 に出力し、表示させ、以後、処理を終了させる。すなわち、この場合には、C D に記録されている音楽データを再生し、H D D 2 1 にコピーする処理が禁止される。

ステップ S 3 1 で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップ S 3 5 に進み、C P U 1 1 は、ステップ S 1 1 で指定されたコピーする曲として選択された曲（選択曲）

の I S R C を C D から取得する。C D に I S R C が記録されていない場合、C P U 1 1 は、その C D の T O C のデータを読み出し、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これを I S R C に代えて用いる。

ステップ S 3 6 において、C P U 1 1 は、ステップ S 3 5 で取得した I S R C (すなわち、選択曲) が期限データベース (図 9) に登録されているか否かを判定する。I S R C が期限データベースに登録されていない場合には、その曲はまだ H D D 2 1 に記録されていないことになるので、ステップ S 3 7 に進み、C P U 1 1 は、その曲の I S R C と現在の日時とを期限データベースに登録する。なお、C P U 1 1 は、この現在の日時として、C P U 3 2 から転送を受けた、アダプタ 2 6 の R T C 3 5 が出力する値を利用する。そして、ステップ S 3 8 において、C P U 1 1 は、その時点における期限データベースのデータを読み出し、アダプタ 2 6 の C P U 3 2 に転送する。C P U 3 2 は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ 3 4 に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップ S 3 2 において、前回保存しておいたハッシュ値として利用される。

次に、ステップ S 3 9 において、C P U 1 1 は、選択曲が期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図 7 のステップ S 1 3 において、選択曲が期限データベースに登録されているか否かの判定を行うときに用いられる。

ステップ S 3 6 において、選択曲の I S R C が期限データベースに登録されていると判定された場合、その選択曲は、少なくとも一

度、HDD 21に登録されたことがある曲であるということになる。そこで、この場合、ステップS 40に進み、CPU 11は、期限データベースに登録されているその選択曲の登録日時より、現在の日時（アダプタ26のRTC 35が出力した現在の日時）が48時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、HDD 21に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているので、その曲を再度コピーさせたとしても、それほど実害がないので、この場合には、HDD 21へのコピーが許容される。そこで、ステップS 41に進み、CPU 11は、期限データベースの日時を、過去の登録日時から現在の日時（RTC 35の出力する日時）に変更させる。そして、ステップS 38に戻り、CPU 11は、再び、期限データベース全体のハッシュ値をCPU 32に計算させ、不揮発性メモリ34に保存させるとともに、ステップS 39において、その曲に対して未登録のフラグを設定する。

一方、ステップS 40において、現在時刻が登録日時より、まだ48時間以上経過していないと判定された場合、その選択曲のHDD 21へのコピーが禁止される。そこで、この場合には、ステップS 42に進み、CPU 11は、その選択曲に対応して登録済みのフラグを設定する。

以上のようにして、期限データベースチェック処理により、選択曲がHDD 21に登録されているか否かを表すフラグが設定される。

図7に戻り、ステップS 13においてCPU 11は、選択曲が期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択曲が登録済みである場合には、ステップS 14に進み、

CPU 11は、ディスプレイ20に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージを表示させる。これにより、使用者は、その曲をHDD21にコピーすることができない理由を知ることができる。

ステップS13において、選択した曲が期限データベースに登録されていないと判定された場合、ステップS15に進み、CPU 11は、ドライブ22を制御し、そこに装着されているCDから音楽データを読み出させる。この音楽データには、図10に示すように、所定の位置にウォーターマークコードが挿入されている。CPU 11は、ステップS16において、音楽データに含まれているウォーターマークコードを抽出し、そのウォーターマークコードがコピー禁止を表しているか否かをステップS17において判定する。ウォーターマークコードがコピー禁止を表している場合には、ステップS18に進み、CPU 11は、インタフェース17を介してディスプレイ20に、例えば、「コピーは禁止されています」のようなメッセージを表示させ、コピー処理を終了させる。

これに対して、ステップS17において、ウォーターマークがコピー禁止を表していないと判定された場合、ステップS19に進み、CPU 11は、音楽データを、例えば、ATRA C(Adaptive Transform Acoustic Coding)3(商標)などの方式で、ソフトウェア処理により圧縮させる。ステップS20において、CPU 11は、予め設定され、メモリ13に記憶されている暗号鍵を用いて、例えば、DES(Data Encryption Standard)方式、FEAL(Fast Encryption Algorithm)方式などの暗号化方法により、音楽データを暗号

化する。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ 26 の CPU 32 により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ 1 だけではなく、それに付随して装着されたハードウェアとしてのアダプタ 26 の CPU 32 と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

次に、ステップ S 21 において、CPU 11 は、暗号化されたデータを HDD 21 に転送し、1つのファイル（コンテンツファイル 161 として）としてファイル名を付けて保存させる。あるいはまた、1つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

この保存処理と、上記した圧縮符号化処理及び暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

さらに、ステップ S 22 において、CPU 11 は、予め定められている RAM 13 に記憶されている保存用鍵（不正な読み出しでは読み出しが困難になるように記憶されている）を使って、上述した DES 方式、FEAL 方式などの方式で、音楽データを暗号化した暗号鍵を暗号化し、HDD 21 の曲データベース（図 5 に示すコンテンツデータベース 114 の利用条件ファイル 162-1 乃至 162-N に対応する）に保存する。

ステップ S 23 において、CPU 11 は、保存したファイルに関する情報、暗号化された暗号鍵、その曲の情報、使用者が GUI を介して入力した曲名の情報の要素を組にして HDD 21 の曲データ

ベースに登録する。そして、ステップS 2 4において、CPU 1 1は、CPU 3 2に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ 3 4に保存させる。

このようにして、例えば、図 1 1に示すような曲データベースが、HDD 2 1上に登録される。この例においては、アイテム 1乃至アイテム 3のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、及びコピー条件（SCMS）が記録されている。

複製されて一定期間が経過すると、再び複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ 1が故障して、HDD 2 1に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD 2 1に記録することができる。

また、例えば、ネットワーク 2を介してHDD 2 1に記録されている期限データベースの内容を共有することもできる。

以上においては、ISRCに対応して複製された日時が記憶されている場合を例として説明したが、コンテンツやCDを識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組合せなど）を利用することもできる。

次に、図 1 2 A、図 1 2 B及び図 1 2 Cに示すフローチャートを参照して、コンテンツ管理プログラム 1 1 1を実行するCPU 1 1

及びメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6のフラッシュメモリ61（例えば、メモリースティック（商標））に、音楽データを移動する処理について説明する。ステップS51において、CPU11は、曲データベース全体のハッシュ値を計算し、ステップS52で、前回CPU32に計算させ、不揮発性メモリ34に保存しておいたハッシュ値と比較する。両者が一致しない場合、CPU11は、ステップS53に進み、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ20に表示させた後、処理を終了させる。この場合の処理は、図8のステップS31乃至ステップS34の処理と同様の処理である。この場合においては、HDD21からポータブルデバイス6への音楽データの移動が実行されないことになる。

次に、ステップS54において、CPU11は、HDD21に形成されている曲データベースから、そこに登録されている曲の情報を読み出し、ディスプレイ20に、選択のためのGUIとして表示させる。使用者は、この選択のためのGUIに基づいて、HDD21からポータブルデバイス6へ移動させる曲を、キーボード18又はマウス19を操作して選択する。次に、ステップS55において、CPU11は、ステップS54で選択された選択曲の再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図13のフローチャートを参照して後述する。

次に、ステップS56において、パーソナルコンピュータ1のCPU11とポータブルデバイス6のCPU53との間において、相互認証処理が行われ、通信用鍵が共有される。

例えば、ポータブルデバイス 6 のフラッシュメモリ 6 1 (又は、EEPROM 6 8) には、マスター鍵 KM が予め記憶されており、パーソナルコンピュータ 1 の RAM 1 3 (又は、HDD 2 1 の所定のファイル) には、個別鍵 KP と ID が予め記憶されているものとする。CPU 5 3 は、CPU 1 1 から、RAM 1 3 に予め記憶されている ID の供給を受け、その ID と自分自身が有するマスター鍵 KM にハッシュ関数を適用して、RAM 1 3 に記憶されているパーソナルコンピュータ 1 の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ 1 とポータブルデバイス 6 の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

あるいはまた、パーソナルコンピュータ 1 の RAM 1 3 に ID とマスター鍵 KMP を予め記憶させておくとともに、ポータブルデバイス 6 のフラッシュメモリ 6 1 にもポータブルデバイス 6 の ID とマスター鍵 KMM を記憶させておく。そして、それぞれの ID とマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきた ID とマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

なお、認証の方法としては、例えば、IOS (International Organization for Standardization) 9 7 9 8 - 2 を利用することができる。

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップ S 5 7 において、CPU 1 1 は、選択曲のファイル名を曲データベースから読み出し、そのファ

イル名の音楽データ（例えば、図7のステップS20の処理で暗号化されている）をHDD21から読み出す。ステップS58において、CPU11は、ステップS57で読み出したデジタル音楽データの圧縮符号化方式（ステップS19の処理）、暗号化方式（ステップS20の処理）、フォーマットなどをポータブルデバイス6のものに変換する処理を実行する。この変換処理の詳細は、図15のフローチャートを参照して後述する。

ステップS59において、CPU11は、ステップS58で変換した音楽データを、ステップS56の相互認証処理により共有した通信用鍵で暗号化し、ポータブルデバイス6にUSBポート23を介して転送する。ステップS60において、ポータブルデバイス6のCPU53は、USBコネクタ56を介してこの伝送されてきた音楽データを受信すると、その音楽データを、そのままフラッシュメモリ61に記憶させる。

ステップS61において、CPU11は、さらに、曲データベースに登録されているその選択曲の再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス6が管理している形式に変換する。ステップS62において、CPU11は、さらに選択曲の曲データベース中に登録されているコピー条件中のSCMS情報を、ポータブルデバイス6の管理する形式に変換する。そして、ステップS63において、CPU11は、ステップS61で変換した再生条件と、ステップS62で変換したSCMS情報を、ポータブルデバイス6に転送する。ポータブルデバイス6のCPU53は、転送を受けた再生条件とSCMS情報を、フラッシュメモリ61に保存する。

ステップS 6 4において、CPU 1 1はまた、選択曲の曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU 1 1が曲データベース中で扱っている形式のまま、ポータブルデバイス6に転送し、フラッシュメモリ6 1に保存させる。

ステップS 6 5において、CPU 1 1は、選択曲の暗号化されている暗号鍵を曲データベースから読み出し、ステップS 6 6において、その暗号鍵をRAM 1 3に保存されている保存用鍵で復号し、通信用鍵で暗号化する。そして、通信用鍵で暗号化した暗号鍵を、CPU 1 1は、ポータブルデバイス6に転送する。

ポータブルデバイス6のCPU 5 3は、ステップS 6 7で、パーソナルコンピュータ1から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ6 1に保存する。

CPU 5 3は、暗号鍵の保存が完了すると、ステップS 6 8において、パーソナルコンピュータ1に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ1のCPU 1 1は、ポータブルデバイス6からこの通知を受けると、ステップS 6 9において、HDD 2 1から、その音楽データのファイルを削除するとともに、曲データベースからその曲の要素の組を削除する。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS 7 0において、CPU 1 1は、アダプタ2 6のCPU 3 2に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ3 4に保存させる。このハッシュ値が、

上述したステップS 5 2において、前回保存しておいたハッシュ値として用いられることになる。

次に、コンテンツ管理プログラム1 1 1を実行するCPU 1 1による、図1 2 AのステップS 5 5における選択曲の再生条件などのチェック処理について説明する。ステップS 8 1において、CPU 1 1は、曲データベースから、各種の条件を読み出す。CPU 1 1は、ステップS 8 2において、ステップS 8 1で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS 8 3に進み、CPU 1 1は、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ2 0に表示させ、処理を終了させる。ステップS 8 2において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップS 8 4に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ2 6のRTC 3 5より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ1の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。CPU 1 1は、この現在日時をCPU 3 2から提供を受けて、ステップS 8 4の判断を自ら行うか、又は、ステップS 8 1で、曲データベースから読み出した再生条件をアダプタ2 6のCPU 3 2に供給し、CPU 3 2に、ステップS 8 4の判定処理を実行させる。

現在日時が再生終了日時を過ぎている場合、ステップS 8 5に進み、CPU 1 1は、選択曲をHDD 2 1から消去するとともに、曲

データベースから、その選択曲の情報を消去する。ステップS 8 6において、CPU 1 1は、CPU 3 2に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ 3 4に保存させる。以後、処理は終了される。したがって、この場合、音楽データの移動が実行されない。

ステップS 8 4において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップS 8 7に進み、CPU 1 1は、その選択曲の再生時課金条件（例えば、再生1回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、CPU 1 1は、ステップS 8 8において、ポータブルデバイス 6と通信し、ポータブルデバイス 6に課金機能が存在するか否かを判定する。ポータブルデバイス 6に課金機能が存在しない場合には、選択曲をポータブルデバイス 6に転送する訳にはいかないので、ステップS 8 9において、CPU 1 1は、例えば、「転送先が課金機能を有しておりません」のようなメッセージをディスプレイ 2 0に表示させ、音楽データの移動処理を終了させる。

ステップS 8 7において再生時課金条件が登録されていないと判定された場合、又は、ステップS 8 8において、ポータブルデバイス 6に課金機能が存在すると判定された場合、ステップS 9 0に進み、CPU 1 1は、選択曲に関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップS 9 1に進み、CPU 1 1は、ポータブルデバイス 6に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス 6が、その再生条件を守

る機能を有していない場合には、ステップS 9 2に進み、CPU 1 1は、例えば、「転送先の装置が再生条件を守る機能を有しておりません」のようなメッセージをディスプレイ2 0に表示させ、処理を終了させる。

ステップS 9 0において、再生条件が登録されていないと判定された場合、又はステップS 9 1において、ポータブルデバイス6が再生条件を守る機能を有している判定された場合、再生条件等のチェック処理が終了され、図1 2 AのステップS 5 6に戻る。

図1 4は、ポータブルデバイス6が管理している（守ることが可能な）再生条件の例を表している。この例においては、アイテム1乃至アイテム3の各曲について、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム2についてのみ登録されており、アイテム1とアイテム3については登録されていない。したがって、アイテム2の曲が選択曲とされた場合、再生回数の再生条件は守ることが可能であるが、アイテム1又はアイテム3の曲が選択曲とされた場合、再生回数の条件は守ることができないことになる。

次に、図1 5のフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1による、図1 2 AのステップS 5 8におけるフォーマット変換処理の詳細について説明する。ステップS 1 0 1において、CPU 1 1は、HDD 2 1に記録されている選択曲のフォーマット（再生条件、使用条件、コピー条件など）を調べる。ステップS 1 0 2において、CPU 1 1は、相手先の機器（今の場合、ポータブルデバイス6）に設定することが可能な条件を調べる。すなわち、CPU 1 1は、ポータブルデバイス6のC

P U 5 3 に設定可能な条件を問い合わせ、その回答を得る。ステップ S 1 0 3 において C P U 1 1 は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップ S 1 0 2 で調べた条件に基づいて決定する。

ステップ S 1 0 4 において、C P U 1 1 は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップ S 1 0 5 に進み、音楽データをポータブルデバイス 6 に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス 6 が守ることができないので、そのようなポータブルデバイス 6 には、音楽データを移動することが禁止されるのである。

ステップ S 1 0 4 において設定可能な条件が存在すると判定された場合、ステップ S 1 0 6 に進み、C P U 1 1 は、その条件を相手先の機能フォーマットの条件に変換する。そして、ステップ S 1 0 7 において、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス 6 は、設定された条件に従って（その条件を守って）、音楽データ再生することが可能となる。

次に、図 1 6 A、図 1 6 B 及び図 1 6 C に示すフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する C P U 1 1 及びメインプログラムを実行する C P U 5 3 による、H D D 2 1 からポータブルデバイス 6 に音楽データをコピーする場合の処理について説明する。この図 1 6 A、図 1 6 B 及び図 1 6 C のステップ S 1 1 1 乃至ステップ S 1 2 7 の処理は、図 1 2 A、図 1 2 B 及び図 1 2 C の H D D 2 1 からポータブルデバイス 6 へ音楽データを移動させる場合のステップ S 5 1 乃至ステップ S 6 7 の処理と同様の処

理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択曲の再生条件とのチェック処理が行われる。さらに、ポータブルデバイス 6 と、パーソナルコンピュータ 1 との間の相互認証処理の後、音楽データが、パーソナルコンピュータ 1 の HDD 2 1 からポータブルデバイス 6 のフラッシュメモリ 6 1 に転送され、保存される。その後、ステップ S 1 2 8 において、パーソナルコンピュータ 1 の CPU 1 1 は、曲データベースのコピー回数カウンタを 1 だけインクリメントする。そして、ステップ S 1 2 9 において、CPU 1 1 は、CPU 3 2 に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ 3 4 に保存させる。

次に、図 1 7 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 及びメインプログラムを実行する CPU 5 3 による、ポータブルデバイス 6 から HDD 2 1 に音楽データを移動する処理について説明する。ステップ S 1 6 1 において、パーソナルコンピュータ 1 の CPU 1 1 は、ポータブルデバイス 6 の CPU 5 3 に対してフラッシュメモリ 6 1 に記憶されている曲の情報の読み出しを要求する。CPU 5 3 は、この要求に対応して、フラッシュメモリ 6 1 に記憶されている曲の情報をパーソナルコンピュータ 1 に送信する。パーソナルコンピュータ 1 の CPU 1 1 は、この情報に基づいて、ディスプレイ 2 0 に、フラッシュメモリ 6 1 に記憶されている曲を選択するための GUI を表示させる。使用者は、キーボード 1 8 又はマウス 1 9 を操作して、その GUI に基づいて、ポータブルデバイス 6 から HDD 2 1 に移動させる曲を指定する。

ステップS 1 6 2において、CPU 1 1は、CPU 5 3との間において、相互認証処理を実行し、通信用鍵を共有する。この処理は、図1 2 AのステップS 5 6における場合と同様の処理である。

次に、ステップS 1 6 3において、CPU 5 3は、フラッシュメモリ 6 1に記憶されている暗号化されている選択曲の音楽データを読み出し、パーソナルコンピュータ 1に転送する。パーソナルコンピュータ 1のCPU 1 1は、ステップS 1 6 4において、ポータブルデバイス 6から転送されてきた音楽データを、1つのファイルとしてファイル名を付けて、HDD 2 1に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

ステップS 1 6 5において、CPU 5 3は、フラッシュメモリ 6 1に記憶されている選択曲の暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ 1に転送する。この暗号鍵は、例えば、図1 2 CのステップS 6 7の処理でフラッシュメモリ 6 1に保存されていたものである。

ステップS 1 6 6において、パーソナルコンピュータ 1のCPU 1 1は、ポータブルデバイス 6から暗号鍵の転送を受けると、それを通信用鍵で復号し、自分自身の保存用鍵で暗号化する。ステップS 1 6 7で、CPU 1 1は、ステップS 1 6 4で保存した音楽データのファイルのファイル名、その曲の情報を使用者がGUIを介して入力した曲名、ステップS 1 6 6で暗号化した暗号鍵などを、HDD 2 1の曲データベースに登録する。そして、ステップS 1 6 8において、CPU 1 1は、その曲データベース全体のハッシュ値を

CPU 32に計算させ、不揮発性メモリ 34に保存させる。

ステップS 169において、パーソナルコンピュータ 1のCPU 11は、ポータブルデバイス 6に対して暗号鍵が保存されたことを通知し、その曲の音楽データの削除を要求する。CPU 53は、パーソナルコンピュータ 1から、その曲の音楽データの削除が要求されてきたとき、ステップS 170において、フラッシュメモリ 61に記憶されているその曲の音楽データを削除する。

次に、コンテンツ管理プログラム 111を実行するCPU 11及びメインプログラムを実行するCPU 53による、ポータブルデバイス 6からHDD 21へ音楽データをコピーする場合の処理について、図 18のフローチャートを参照して説明する。この図 18に示すステップS 181乃至ステップS 188の処理は、図 17のポータブルデバイス 6からHDD 21へ音楽データを移動させる場合の処理におけるステップS 161乃至ステップS 168の処理と同様の処理である。すなわち、コピー処理の場合は、図 17のステップS 169、S 170の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

次に、図 19のフローチャートを参照して、EMDサーバ 4及びコンテンツ管理プログラム 111を実行するCPU 11による、EMDサーバ 4から転送を受けた音楽データをHDD 21にコピーする処理について説明する。ステップS 201において、CPU 11は、キーボード 18又はマウス 19を介して使用者からEMDサーバ 4へのアクセスが指令されたとき、通信部 25を制御し、ネットワーク 2を介してEMDサーバ 4にアクセスさせる。EMDサーバ 4は、このアクセスに対応して、自分自身が保持している曲の曲番

号、曲名、各情報などの情報を、ネットワーク 2 を介してパーソナルコンピュータ 1 に転送する。パーソナルコンピュータ 1 の CPU 11 は、通信部 25 を介して、この情報を取得したとき、それをインタフェース 17 を介してディスプレイ 20 に表示させる。使用者は、ディスプレイ 20 に表示された GUI を利用して、ステップ S202 において、コピーを希望する曲を指定する。この指定情報は、ネットワーク 2 を介して EMD サーバ 4 に転送される。ステップ S203 において、CPU 11 は、EMD サーバ 4 との間において、ネットワーク 2 を介して相互認証処理を実行し、通信用鍵を共有する。

パーソナルコンピュータ 1 と EMD サーバ 4 との間で行われる相互認証処理は、例えば、ISO 9798-3 で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ 1 は、自分自身の機密鍵と EMD サーバ 4 の公開鍵を予め有しており、EMD サーバ 4 は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ 1 の公開鍵は、EMD サーバ 4 から転送したり、あるいはパーソナルコンピュータ 1 に予め配布されている証明書(certificate)をパーソナルコンピュータ 1 から EMD サーバ 4 に転送し、その証明書を EMD サーバ 4 が確認し、公開鍵を得るようにしてもよい。さらに、ステップ S204 において、CPU 11 は、EMD サーバ 4 との間において課金に関する処理を実行する。この課金の処理の詳細は、図 20 のフローチャートを参照して後述する。

次に、ステップ S205 において、EMD サーバ 4 は、パーソナルコンピュータ 1 に対して、ステップ S202 で指定された曲の暗

号化されている音楽データをネットワーク 2 を介してパーソナルコンピュータ 1 に転送する。このとき、時刻情報も適宜転送される。ステップ S 2 0 6 において、CPU 1 1 は、転送を受けた音楽データをファイル名を付けて HDD 2 1 に 1 つのファイルとして保存する。ステップ S 2 0 7 において、EMD サーバ 4 は、さらに、その曲の暗号鍵をステップ S 2 0 3 でパーソナルコンピュータ 1 と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ 1 へ転送する。

CPU 1 1 は、ステップ S 2 0 8 において、EMD サーバ 4 より転送を受けた暗号鍵を単独で、又はアダプタ 2 6 の CPU 3 2 と共同して通信用鍵を用いて復号し、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化する。ステップ S 2 0 9 において、CPU 1 1 は、その曲のファイル名、曲の情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD 2 1 の曲データベースに登録する。さらに、ステップ S 2 1 0 において、CPU 1 1 は、その曲データベース全体のハッシュ値を CPU 3 2 に計算させ、不揮発性メモリ 3 4 に保存させる。

なお、ステップ S 2 0 5 において EMD サーバ 4 は、音楽データとともに、時刻データをパーソナルコンピュータ 1 に送信する。この時刻データは、パーソナルコンピュータ 1 からアダプタ 2 6 に転送される。アダプタ 2 6 の CPU 3 2 は、パーソナルコンピュータ 1 より転送されてきた時刻データを受信すると、ステップ S 2 1 1 において、RTC 3 5 の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ 2 6 の RTC 3 5 の時刻情報を修正する。

ようにしたので、アダプタ 26 を常に正しい時刻情報を保持することが可能となる。

次に、図 20 のフローチャートを参照して、EMD サーバ 4 及びコンテンツ管理プログラム 111 を実行する CPU 11 による、図 19 のステップ S 204 における課金に関する処理の詳細について説明する。ステップ S 221 において、パーソナルコンピュータ 1 の CPU 11 は、ステップ S 201 で EMD サーバ 4 から伝送されてきた価格情報の中から、ステップ S 202 で指定された選択曲の価格情報を読み取り、これを HDD 21 上の課金ログに書き込む。図 21 は、このような課金ログの例を表している。この例においては、使用者は、アイテム 1 乃至アイテム 3 を、EMD サーバ 4 からコピーしており、アイテム 1 とアイテム 2 の領域は 50 円とされ、アイテム 3 の料金は 60 円とされている。その時点における課金ログのハッシュ値も、CPU 32 により計算され、不揮発性メモリ 34 に登録されている。

次に、ステップ S 222 において、パーソナルコンピュータ 1 の CPU 11 は、ステップ S 221 で書き込んだ課金ログを HDD 21 から読み出し、これをネットワーク 2 を介して EMD サーバ 4 に転送する。EMD サーバ 4 は、ステップ S 223 において、パーソナルコンピュータ 1 から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMD サーバ 4 は、内蔵するデータベースに、パーソナルコンピュータ 1 の使用者から伝送されてきた課金ログを追加更新する。そして、ステップ S 224 において、EMD サーバ 4 は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップ S 225 に進み、EMD サーバ

4は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップS 2 2 6において、決裁サーバは、パーソナルコンピュータ1の使用者に対する決裁処理を実行する。ステップS 2 2 4において、決裁は直ちには行われないと判定された場合、ステップS 2 2 5とS 2 2 6の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

次に、図2 2 A及び図2 2 Bに示すフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1による、音声入出力インタフェース2 4のIEC 6 0 9 5 8端子から入力された、図示せぬCDプレーヤなどからの再生音楽データを、HDD 2 1にコピーする場合の処理について説明する。ステップS 2 4 1において、使用者は、CDプレーヤのIEC 6 0 9 5 8出力端子を、パーソナルコンピュータ1の音声入出力インタフェース2 4のIEC 6 0 9 5 8端子に接続する。ステップS 2 4 2において、使用者は、キーボード1 8又はマウス1 9を操作し、CDプレーヤからコピーする曲の曲名（又は、曲に対応する番号）を入力する。そして、ステップS 2 4 3において使用者は、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1のキーボード1 8又はマウス1 9を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

CDプレーヤにおいて、CDの再生が開始されると、ステップS 2 4 4において、CDプレーヤから出力された音楽データが、IE

C 6 0 9 5 8 端子を介してパーソナルコンピュータ 1 に転送されてくる。ステップ S 2 4 5 において、CPU 1 1 は、I E C 6 0 9 5 8 端子を介して入力されてくるデータから、S C M S (Serial Copy Management System) データを読み取る。この S C M S データには、コピー禁止、コピー 1 回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップ S 2 4 6 において、CPU 1 1 は、S C M S データがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップ S 2 4 7 に進み、CPU 1 1 は、ディスプレイ 2 0 に、例えば、「コピーが禁止されています」といったメッセージを表示させ、コピー処理を終了する。すなわち、この場合には、H D D 2 1 へのコピーが禁止される。

CPU 1 1 は、ステップ S 2 4 6 において、ステップ S 2 4 5 で読み取った S C M S 情報がコピー禁止を表していないと判定した場合、ステップ S 2 4 8 に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップ S 2 4 9 において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップ S 2 4 7 に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

ステップ S 2 4 9 において、ウォータマークがコピー禁止を表していないと判定された場合、ステップ S 2 5 0 に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択曲が既に登録されていれば、ステップ S 2 5 1, S 2 5 2 の処理で、処理が終了される。この処理は、図 7 のステップ S 1 3, S 1 4 の処理と同様の処理である。

選択曲がまだ H D D 2 1 に登録されていない曲であれば、ステッ

ブS 2 5 3乃至S 2 5 8で、その登録処理が実行される。このステップS 2 5 3乃至ステップS 2 5 8の処理は、ステップS 2 5 7において、I E C 6 0 9 5 8端子から供給されてくるS C M S情報も曲データベースに登録される点を除き、図7のステップS 1 9乃至ステップS 2 4の処理と同様の処理であるので、その説明は省略する。

次に、図2 3 A及び図2 3 Bに示すフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するC P U 1 1による、音楽データをH D D 2 1からI E C 6 0 9 5 8端子に出力（再生）する場合の処理について説明する。ステップS 2 7 1乃至ステップS 2 7 3において、図1 6 AのステップS 1 1 1乃至S 1 1 3における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップS 2 7 4に進み、C P U 1 1は、H D D 2 1の曲データベースにアクセスし、そこに登録されている曲の情報を読み出し、ディスプレイ2 0に表示させる。使用者は、その表示を見て、キーボード1 8又はマウス1 9を適宜操作して、再生出力する曲を選択する。ステップS 2 7 5において、C P U 1 1は、選択曲の再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図2 4のフローチャートを参照して後述する。

次に、ステップS 2 7 6において、C P U 1 1は、ステップS 2 7 4において選択された曲の暗号鍵を曲データベースから読み出し、保存用鍵で復号する。ステップS 2 7 7において、C P U 1 1は、

選択曲のSCMS情報を曲データベースから読み出し、IEC60958端子から出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は1だけインクリメントされ、新たなSCMS情報とされる。ステップS278において、CPU11はさらに、選択曲のISRCを曲データベースから読み出す。

次に、ステップS279において、CPU11は、曲データベースから選択曲ファイル名を読み出し、そのファイル名を基に、その音楽データをHDD21から読み出す。CPU11はさらに、その音楽データに対応する暗号鍵を曲データベースから読み出し、保存用鍵で復号し、復号した暗号鍵を用いて、暗号化されている音楽データを復号する。CPU11は、さらに、その音楽データの圧縮符号を復号する。ステップS280において、CPU11は、ステップS279で、復号したデジタル音楽データを、ステップS277で決定したSCMS情報、並びにステップS278で読み出したISRC情報とともに、IEC60958の規定に従って、IEC60958端子から出力する。さらにまた、デジタル音楽データをアナログ化し、音声入出力インタフェース24のアナログ出力端子から出力する。

ステップS281において、CPU11は、曲データベース中の再生回数カウンタの値を1だけインクリメントする。そして、ステップS282において、選択曲に再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS283に進み、CPU11は、対応する料金を課金ログに書き込み、ステップS284において、曲データベース全体のハッ

シュ値をCPU 32に計算させ、不揮発性メモリ34に記憶させる。ステップS 282において、選択曲に再生時課金条件が付加されていないと判定された場合、ステップS 283とステップS 284の処理はスキップされる。

次に、図24のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU 11による、図23AのステップS 275の再生条件等のチェック処理の詳細について説明する。ステップS 301において、CPU 11は、曲データベースの各種条件を読み出す。ステップS 302においてCPU 11は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップS 303に進み、選択曲をHDD 21から削除させるとともに、曲データベースから選択曲の情報を削除させる。ステップS 304において、CPU 11はさらに、曲データベースの新たなハッシュ値をCPU 32に計算させ、そのハッシュ値を不揮発性メモリ34に保存させる。この場合、再生出力は禁止される。

ステップS 302において、再生回数が制限回数を過ぎていないと判定された場合、ステップS 305に進み、CPU 11は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップS 303において、選択曲をHDD 21から削除させるとともに、曲データベースからも削除させる。そして、ステップS 304において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

ステップS 305において、再生終了日時が現在日時を過ぎてい

ないと判定された場合は、ステップS 3 0 6に進み、CPU 3 2は、その選択曲に対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS 3 0 7に進み、CPU 1 1は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ2 0に表示させる。ステップS 3 0 6において、再生時課金条件が付加されていないと判定された場合、ステップS 3 0 7の処理はスキップされる。

次に、図2 5 A及び図2 5 Bに示すフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1及びメインプログラムを実行するCPU 5 3による、HDD 2 1からポータブルデバイス6経由で音楽データを出力（再生）する場合の処理について説明する。ステップS 3 2 1乃至ステップS 3 2 5において、曲データベースの改竄チェックと選択曲の指定、並びに選択曲の再生条件等のチェック処理が行われる。その処理は、図2 3 AのステップS 2 7 1乃至ステップS 2 7 5の処理と同様の処理であるので、その説明は省略する。

ステップS 3 2 6において、ポータブルデバイス6とパーソナルコンピュータ1の間で相互認証処理が実行され、相互の間で、通信鍵が共有される。ステップS 3 2 7において、パーソナルコンピュータ1のCPU 1 1は、ポータブルデバイス6に対して、これから送る暗号化音声データを再生するように命令する。ステップS 3 2 8において、CPU 1 1は、ステップS 3 2 4で指定された選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データをHDD 2 1から読み出す。CPU 1 1は、ステップS 3 2 9において、音楽データの圧縮符号化方式、暗号化方式、フォ

ーマットなどをポータブルデバイス6の方式のものに変換する処理を実行する。そして、ステップS330において、CPU11は、ステップS329において変換した音楽データを通信用鍵で暗号化し、ポータブルデバイス6に転送する。

ステップS331において、ポータブルデバイス6のCPU53は、ステップS327において、パーソナルコンピュータ1から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップS332において、CPU11は、曲データベースの再生回数カウントを1だけインクリメントする。さらに、ステップS333において、CPU11は、選択曲に再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップS334において、その料金を課金ログに書き込み、ステップS335において、CPU32に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択曲に再生時課金条件が付加されていない場合には、ステップS334，ステップS335の処理はスキップされる。

本発明においては、音楽データが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU11を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

さらに、上述したように、CPU11の機能の一部は、ハードウェアとしてのアダプタ26に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

例えば、上述したように、曲データベースのハッシュ値は、曲デ

ータベース自体に保存されるのではなく、アダプタ 26 の不揮発性メモリ 34 に保存される。すなわち、図 8 のステップ S 32, S 33 などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 34 に記憶されているものとされる。これにより、例えば、HDD 21 に保存されている音楽データを、他の記録媒体にコピー又は移動させる前に、HDD 21 の記録内容をバックアップしておき、HDD 21 から、そこに保存されている音楽データを他の記録媒体にコピー又はムーブした後、HDD 21 にバックアップしておいたデータを再びリストアするようにすることで、実質的に再現なく、コピー又はムーブができてしまうようなことが防止される。

例えば、図 26 に示すように、HDD 21 に曲 A, B が保存されている場合、不揮発性メモリ 34 には、曲 A と曲 B の情報に対応するハッシュ値が保存されている。この状態において、HDD 21 の記録データを他の記録媒体 251 にバックアップしたとする。その後、HDD 21 に保存されている曲 A と曲 B のうち、曲 A を他の記録媒体 252 に移動させた場合、その時点において、HDD 21 に記録されている曲は、曲 B だけとなるので、不揮発性メモリ 34 のハッシュ値も、曲 B に対応するハッシュ値に変更される。

したがって、その後、記録媒体 251 にバックアップしておいた HDD 21 の内容を HDD 21 にリストアして、HDD 21 に、再び曲 A と曲 B を保存させたとしても、不揮発性メモリ 34 には、曲 B の情報から演算されたハッシュ値が記憶されており、曲 A と曲 B の情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 21 に記憶されている曲 A と曲 B に基づ

くハッシュ値が、不揮発性メモリ 34 に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 21 に保存されている曲 A と曲 B の利用が制限されてしまうことになる。

さらに、上述したように、アダプタ 26 は、RTC 35 を内蔵しており、この RTC 35 の値は、正しい認証結果が得られた他の装置（例えば、EMD サーバ 4）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ 1 が管理するものではなく、RTC 35 が出力するものが利用される。したがって、使用者が、パーソナルコンピュータ 1 の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

また、アダプタ 26 は、暗号化されて転送されてきたプログラムを ROM 36 に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図 27 のフローチャートを参照して説明する。

すなわち、パーソナルコンピュータ 1 は、アダプタ 26 に対して、所定の処理を実行させたいとき、ステップ S 351 において、アダプタ 26 に実行させるべきプログラムを RAM 13 に予め記憶されている暗号鍵を用いて暗号化してアダプタ 26 に転送する。アダプタ 26 の ROM 36 には、パーソナルコンピュータ 1 から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU 32 は、この ROM 36 に記憶されているプログラムに従って、パーソナルコンピュータ 1 から転送されてきた暗号化されているプログラムをステップ S 352

において復号する。そして、ステップS 3 1 3において、CPU 3 2は、復号したプログラムをRAM 3 3に展開し、ステップS 3 5 4において、そのプログラムを実行する。

例えば、上述したように、パーソナルコンピュータ1のCPU 1 1は、HDD 2 1の曲データベースのハッシュ値をアダプタ2 6に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ2 6のCPU 3 2に転送する。CPU 3 2は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ3 4に記憶させる。あるいは、そのハッシュ値を、CPU 3 2は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ1のCPU 1 1に転送する。

図2 8は、アダプタ2 6の内部のより具体的な構成を表している。アダプタ2 6は、半導体ICとして形成される。アダプタ2 6は、図3に示したインタフェース3 1、CPU 3 2、RAM 3 3、不揮発性メモリ3 4、RTC 3 5、ROM 3 6以外に、RAM 3 3に対する書き込みと読み出しを制御するRAMコントローラ2 6 1、並びに論理回路2 6 2を有している。論理回路2 6 2は、例えば、暗号化されている音楽データを解読した後、解読したデータをアダプタ2 6から直接出力するような場合の処理のために用いられる。

これらのインタフェース3 1乃至ROM 3 6、RAMコントローラ2 6 1、並びに論理回路2 6 2は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

水晶振動子2 7 1は、アダプタ2 6が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路

272は、RTC35を動作させるための発振回路である。バッテリー273は、発振回路272、不揮発性メモリ34、及びRTC35に対してバックアップ用の電力を供給している。アダプタ26のその他の回路には、パーソナルコンピュータ1の電源供給回路281からの電力が供給されている。

不揮発性メモリ34は、書き込み消去可能なROMで構成することも可能であるが、バッテリー273からのバックアップ電源でバックアップされるRAMで構成する場合には、例えば、図29A及び図29Bに示すように、不揮発性メモリ34の上に保護アルミニウム層291を形成し、さらに、その保護アルミニウム層291と同一平面上となるように、不揮発性メモリ34にバッテリー273からの電力を供給する電源パターン292を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ34を改竄すべく、保護アルミニウム層291を削除しようとする、同一平面上の電源パターン292も削除されてしまい、不揮発性メモリ34に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

さらに、図30に示すように、不揮発性メモリ34に対するデータの書き込み又は読み出しのための配線301-1乃至301-3は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線301-3からデータを読み出すためには、上方の配線301-1、301-2を除去しなければならず、複数の配線301-1、301-2、301-3から同時にデータを読み取ることができなくなる。さらにまた、この配

線 3 0 1 - 1 乃至 3 0 1 - 3 を冗長に形成し、直接プローブすると、その付加容量により、その内容を解析することが困難になるようにすることができる。

以上においては、記録媒体として、ポータブルデバイス 6 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転又はコピーする場合にも応用することが可能である。

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

以上のように、本発明によれば、次のような効果を奏することができる。

(1) HDD 2 1 に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上で HDD 2 1 に記録するようにしたので、HDD 2 1 に記録されている音楽データをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

(2) 所定の曲を 1 回コピーしたとき、一定時間（上記例の場合、4 8 時間）の間、その曲をコピーすることができないようにするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

さらにデータベースを更新するたびに、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

(3) 外部の装置に音楽データを渡したら、HDD 2 1 上の音楽データを消去するようにしたので、HDD 2 1 内に元のデジタル

音楽データが残らず、その複製を大量に配布することが防止される。

(4) HDD 2 1 内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD 2 1 の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータを HDD 2 1 にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

(5) パーソナルコンピュータ 1 が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

(6) 外部機器から、パーソナルコンピュータ 1 に対してデータを渡す前に、パーソナルコンピュータ 1 のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対して音楽データを渡してしまうようなことが防止される。

(7) 曲の同一性の判定に I S R C を用い、I S R C が取得できないときは、T O C を用いるようにしたので、I S R C が取得できなくとも、曲の同一性を判定することが可能になる。

(8) パーソナルコンピュータ 1 におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ 1 に外付けされるアダプタ 2 6 に負担させるようにしたので、パーソナルコンピュータ 1 のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

なお、アダプタ 2 6 が実行する処理は、セキュアなプログラムで CPU 1 1 が実行するようにしてもよい。この場合において、パー

ソナルコンピュータ 1 は、アダプタ 2 6 の R T C 3 5 が供給する現在時刻に代えて、ネットワーク 2 に接続されている特定のサーバ（例えば、E M D 登録サーバ 3）から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ 1 は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けないようにしてもよい。

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、又は、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図 3 に示すように、磁気ディスク 4 1（フロッピディスクを含む）、光ディスク 4 2（C D - R O M (Compact Disc-Read Only Memory)、D V D (Digital Versatile Disc)を含む）、光磁気ディスク 4 3（M D (Mini-Disc)を含む）、若しくは半導体メモリ 4 4 などよりなるパッケージメディア、又は、プログラムが一時的若しくは永続的に格納される R O M 1 2 や、H D D 2 1 などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部 2 5 などのインタフェースを介して、ローカルエリアネットワーク

又はインターネットなどのネットワーク 2、デジタル衛星放送といった、有線又は無線の通信媒体を利用して行われる。

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

本発明に係る情報処理装置、情報処理方法及びプログラム格納媒体によれば、コンテンツの識別情報に対応させて複製されたときの時間情報を記憶するようにしたので、ユーザの利益を大きく損なうことなく、大量の複製を実質的に禁止することができるようになる。

請求の範囲

1. コンテンツを識別する識別情報と、前記識別情報に対応して、前記コンテンツが複製されたときの時刻情報を記憶する記憶手段と、複製しようとするコンテンツの識別情報を取得する取得手段と、前記取得手段により取得された前記識別情報と、前記記憶手段に記憶されている前記時刻情報に対応して、前記コンテンツを複製する複製手段と

を含むことを特徴とする情報処理装置。

2. コンテンツを識別する識別情報と、前記識別情報に対応して、前記コンテンツが複製されたときの時刻情報を記憶する記憶ステップと、

複製しようとするコンテンツの識別情報を取得する取得ステップと、

前記取得ステップで取得された前記識別情報と、前記記憶ステップで記憶された前記時刻情報に対応して、前記コンテンツを複製する複製ステップと

を含むことを特徴とする情報処理方法。

3. コンテンツを識別する識別情報と、前記識別情報に対応して、前記コンテンツが複製されたときの時刻情報を記憶する記憶ステップと、

複製しようとするコンテンツの識別情報を取得する取得ステップと、

前記取得ステップで取得された前記識別情報と、前記記憶ステッ

ブで記憶された前記時刻情報に対応して、前記コンテンツを複製する複製ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

補正書の請求の範囲

[2000年5月26日(26.05.00)国際事務局受理:新しい請求の
範囲4-14が加えられた;他の請求の範囲は変更なし。(4頁)]

1. コンテンツを識別する識別情報と、前記識別情報に対応して、
前記コンテンツが複製されたときの時刻情報を記憶する記憶手段と、
複製しようとするコンテンツの識別情報を取得する取得手段と、
前記取得手段により取得された前記識別情報と、前記記憶手段に
記憶されている前記時刻情報に対応して、前記コンテンツを複製す
る複製手段と

を含むことを特徴とする情報処理装置。

2. コンテンツを識別する識別情報と、前記識別情報に対応して、
前記コンテンツが複製されたときの時刻情報を記憶する記憶ステッ
プと、

複製しようとするコンテンツの識別情報を取得する取得ステップ
と、

前記取得ステップで取得された前記識別情報と、前記記憶ステッ
プで記憶された前記時刻情報に対応して、前記コンテンツを複製す
る複製ステップと

を含むことを特徴とする情報処理方法。

3. コンテンツを識別する識別情報と、前記識別情報に対応して、
前記コンテンツが複製されたときの時刻情報を記憶する記憶ステッ
プと、

複製しようとするコンテンツの識別情報を取得する取得ステップ
と、

前記取得ステップで取得された前記識別情報と、前記記憶ステッ

補正された用紙(条約第19条)

ブで記憶された前記時刻情報に対応して、前記コンテンツを複製する複製ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

4. (追加) 上記コンテンツは情報記憶媒体から再生されることを特徴とする請求の範囲第2項記載の情報処理方法。

5. (追加) 上記情報記憶媒体は音楽情報を記憶するコンパクトディスクであることを特徴とする請求の範囲第4項記載の情報処理方法。

6. (追加) 上記コンテンツを識別する識別情報は I S R C (International Standard Recording Code) であることを特徴とする請求の範囲第2項記載の情報処理方法。

7. (追加) 上記コンテンツを識別する識別情報は T O C (Table of Contents) であることを特徴とする請求の範囲第2項記載の情報処理方法。

8. (追加) 上記記憶ステップにおいて、上記コンテンツを識別する識別情報として I S R C (International Standard Recording Code) を情報記憶媒体より読み出すようになし、上記情報記憶媒体に I S R C が記憶されていない場合は、T O C (Table of Contents) のデータを上記識別情報として利用することを特徴とする請求の範囲第2項記載の情報処理方法。

9. (追加) 上記記憶ステップにより上記識別情報と上記時刻情報に対応して期限データベースに記憶されることを特徴とする請求の範囲第2項記載の情報処理方法。

10. (追加) 期限データベース内のデータをチェックするチェッ

クステップをさらに有し、該チェックステップはハッシュ関数を用いて改竄が検知されるようになすことをことを特徴とする請求の範囲第9項記載の情報処理方法。

11. (追加) 上記複製ステップは、さらに、上記取得ステップにおいて取得された上記コンテンツの上記識別情報が過去に上記記憶ステップにおいて記憶されていることが検知されたとき、該記憶されたコンテンツの時刻情報から現在の時刻情報を比較し、所定時間以上経過しているか否かを判定する判定ステップを有することを特徴とする請求の範囲第2項記載の情報処理方法。

12. (追加) 上記判定ステップにおける判定の結果、上記所定時間経過していないと判断された場合は複製を禁止するようになすことを特徴とする請求の範囲第11項記載の情報処理方法。

13. (追加) 上記判定ステップにおける判定の結果、上記所定時間経過していないと判断された場合は、上記コンテンツ内のウォーターマークを検知し、該ウォーターマークに基づいて複製処理を行うことを特徴とする請求の範囲第11項記載の情報処理方法。

14. (追加) 過去に複製を行ったコンテンツを識別する識別コードと、上記コンテンツが複製された時刻データが対応付けられて記憶されるデータベースを有する情報処理装置に用いられる情報処理方法であって、

これから複製を行おうとするコンテンツの識別コードを取得する取得ステップと、

前記取得ステップで取得された前記識別コードが上記データベースに既に記憶されているか否かを判断する判断ステップと、

該判断ステップにより上記識別コードが上記データベースに既に

記憶されていると判断された時、上記データベース内に上記識別コード対応付けて記憶されている時刻データと現在の時刻情報とを比較する比較ステップと、

該比較ステップにより上記記憶されている時刻データより現在の時刻が所定時間以上経過しているか否かを判定する判定ステップとを有し、

該判定ステップの結果、所定時間以上経過していないと判断された場合は上記コンテンツの複製を禁止するようになすことを特徴とする情報処理方法。

1/36

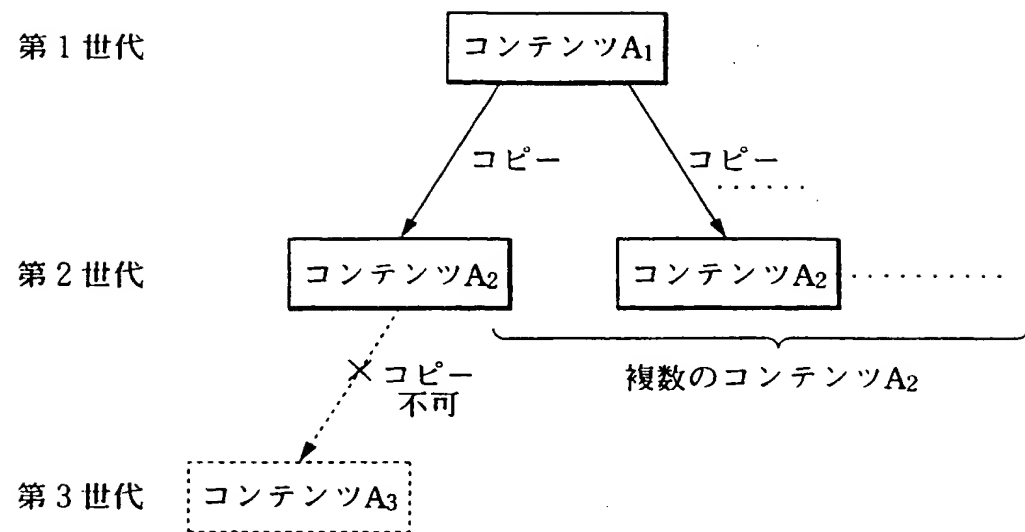


FIG.1

2/36

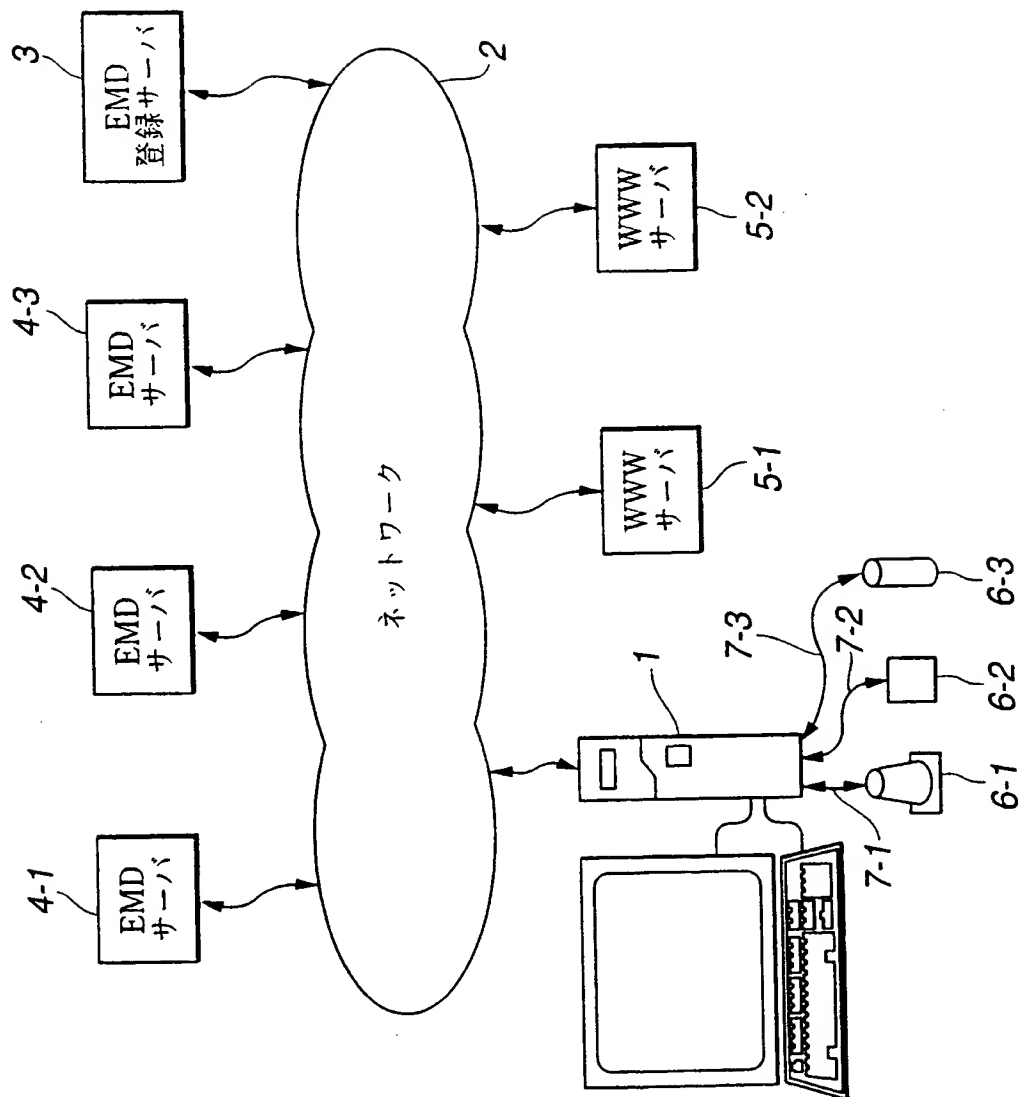


FIG.2

3/36

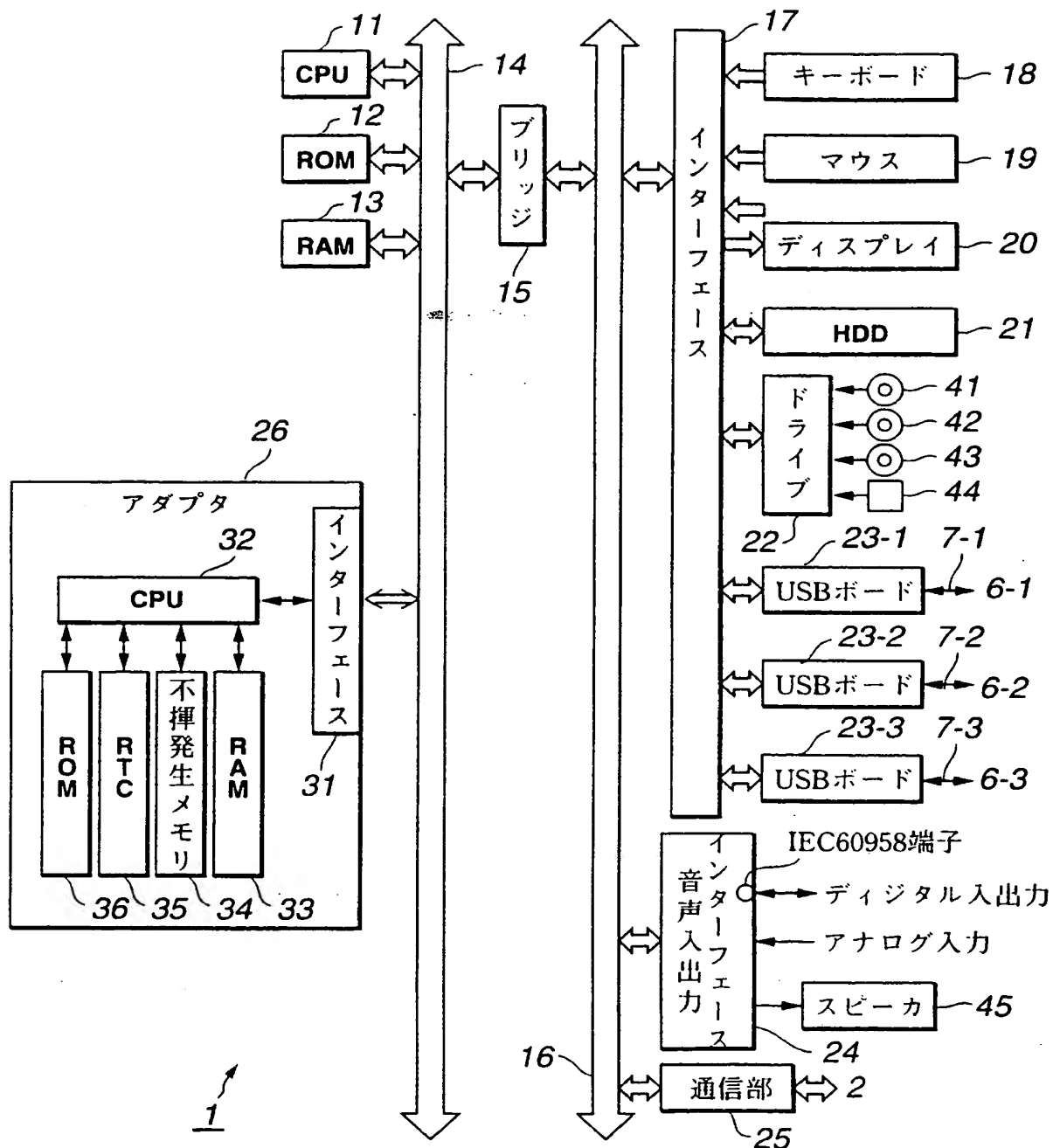


FIG.3

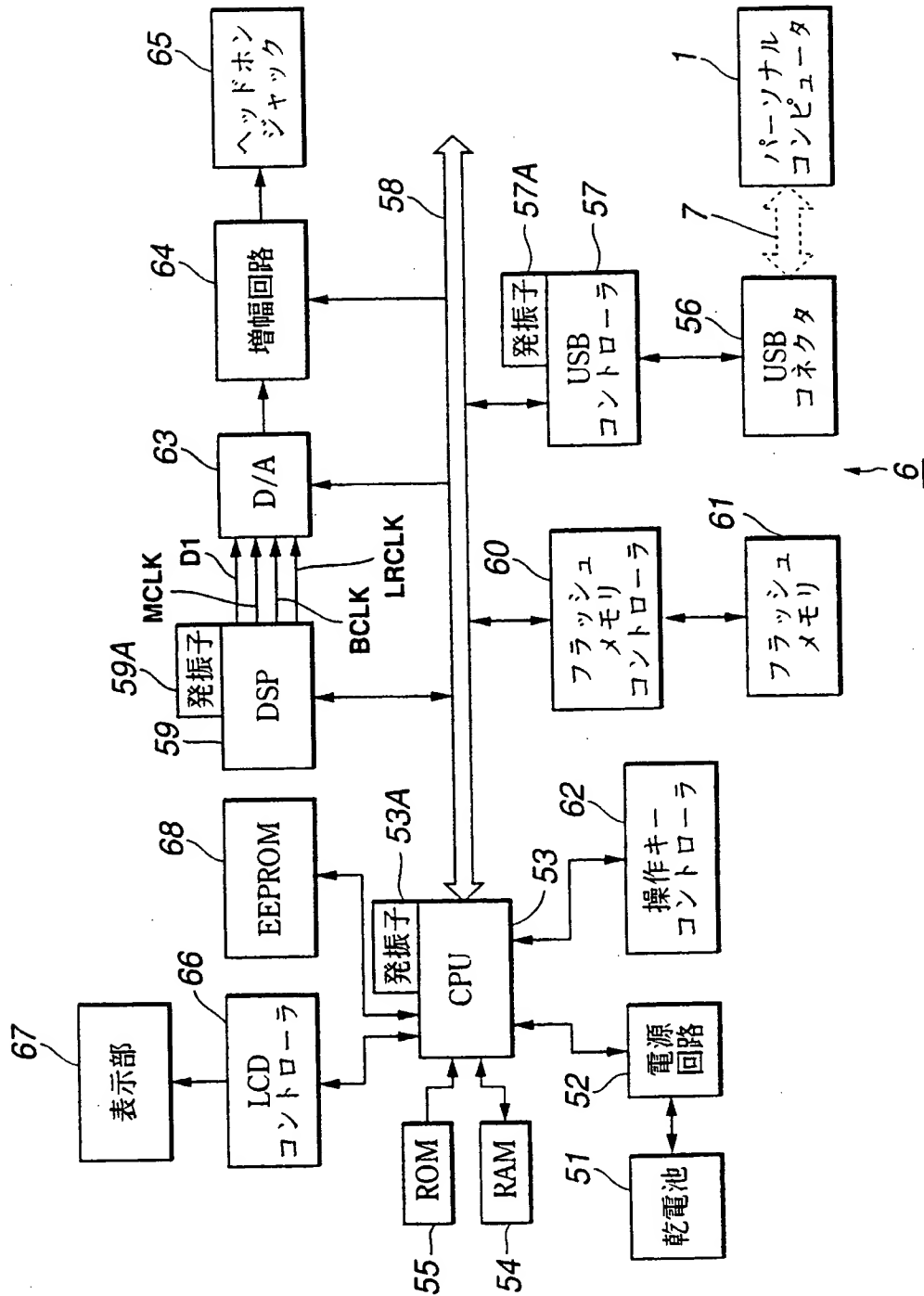


FIG.4

5/36

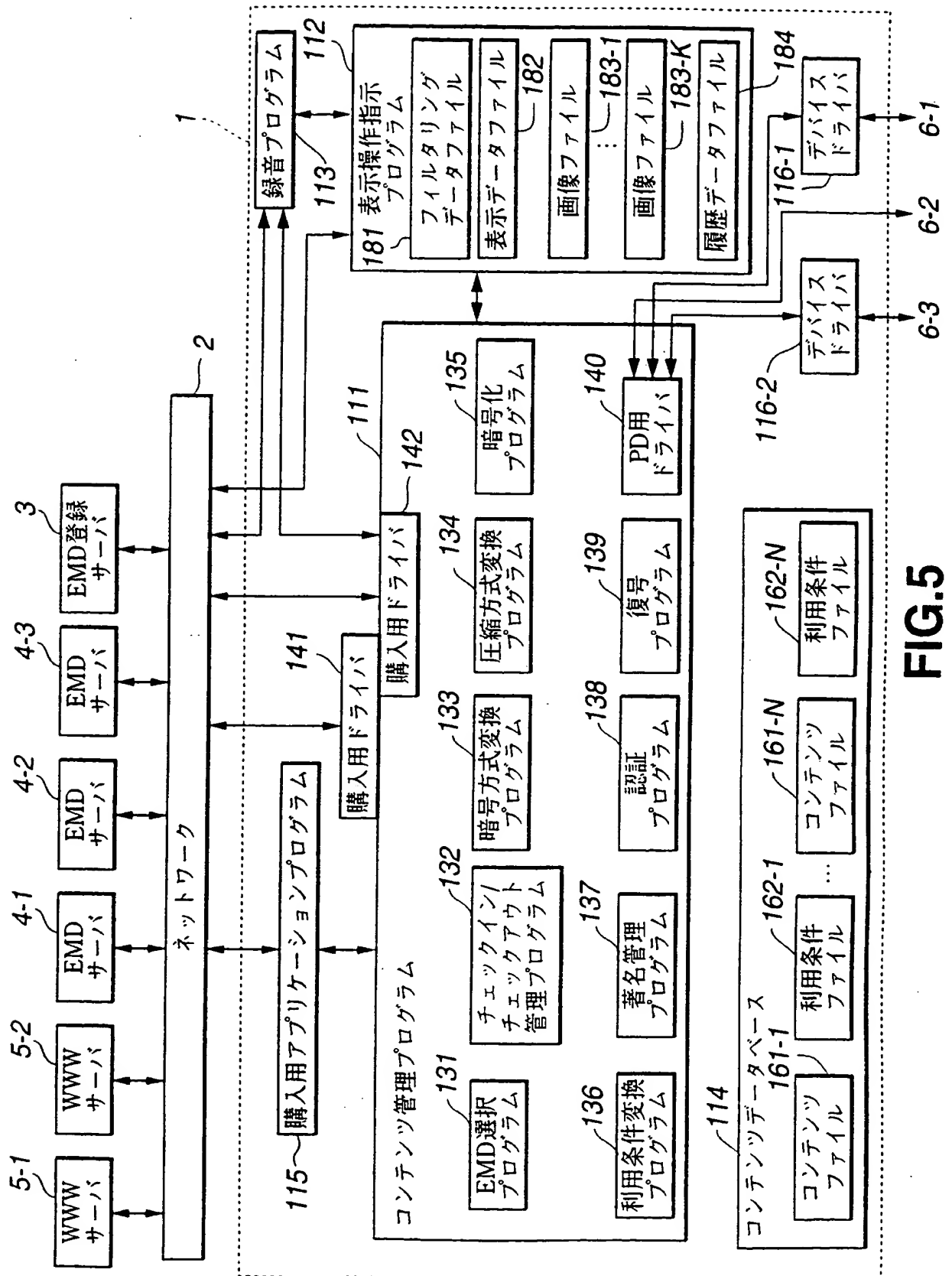


FIG. 5

6/36

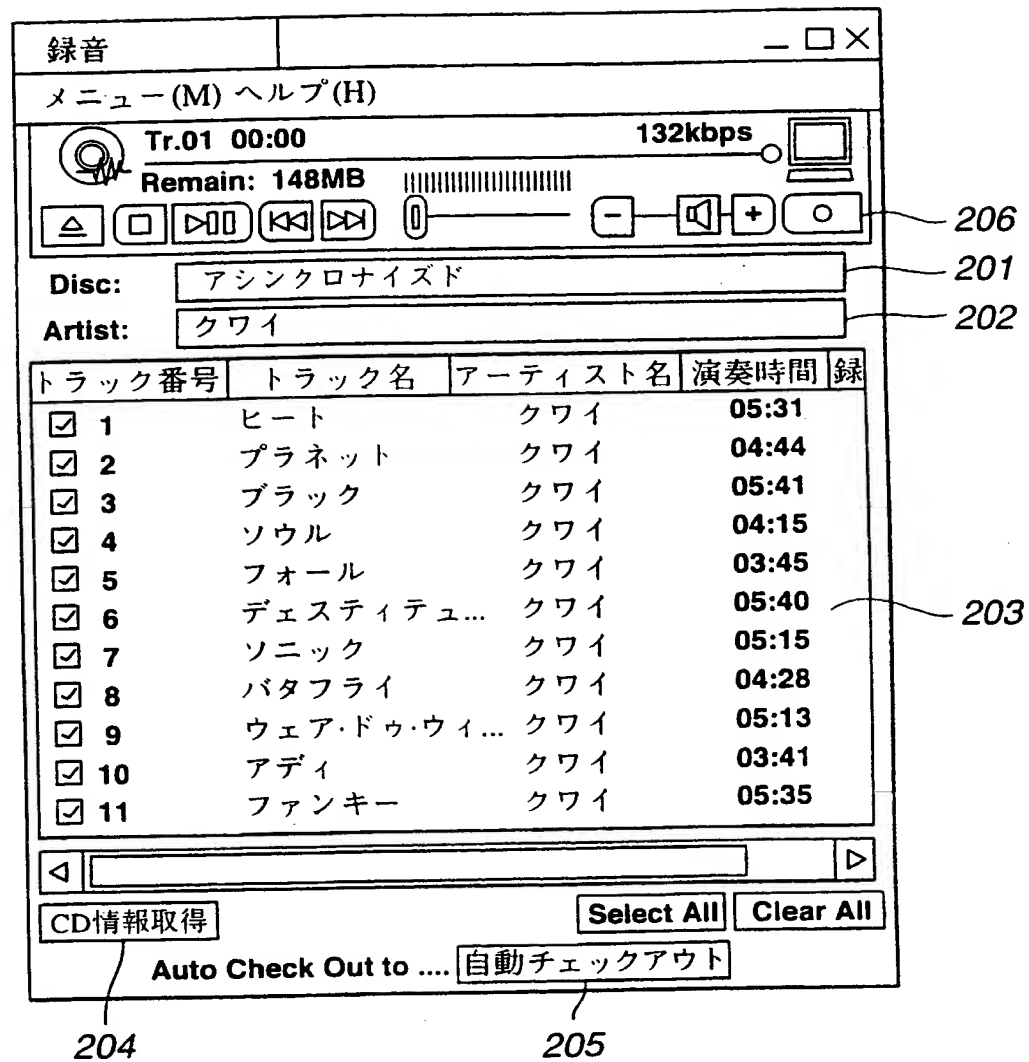


FIG.6

7/36

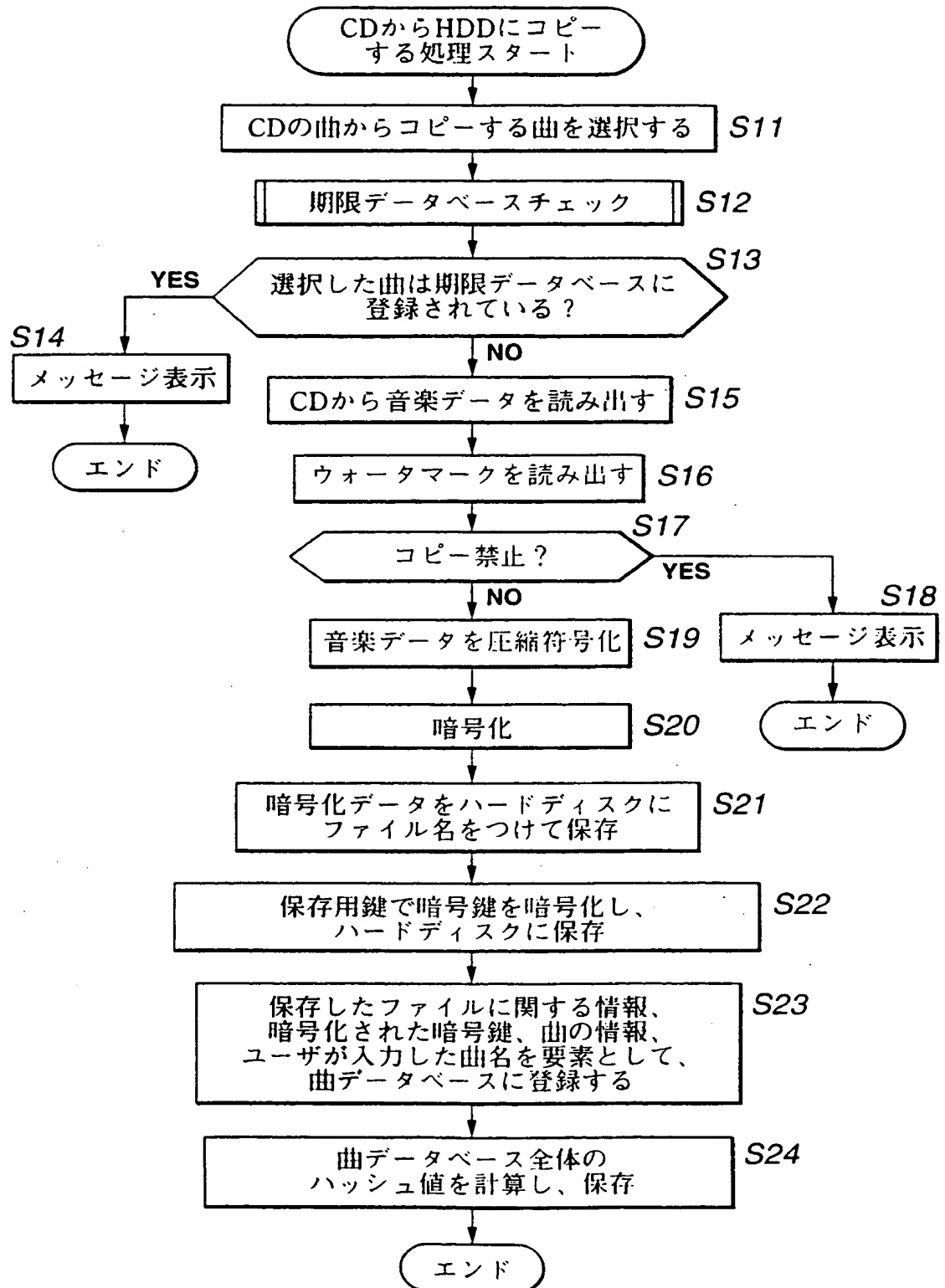


FIG.7

8/36

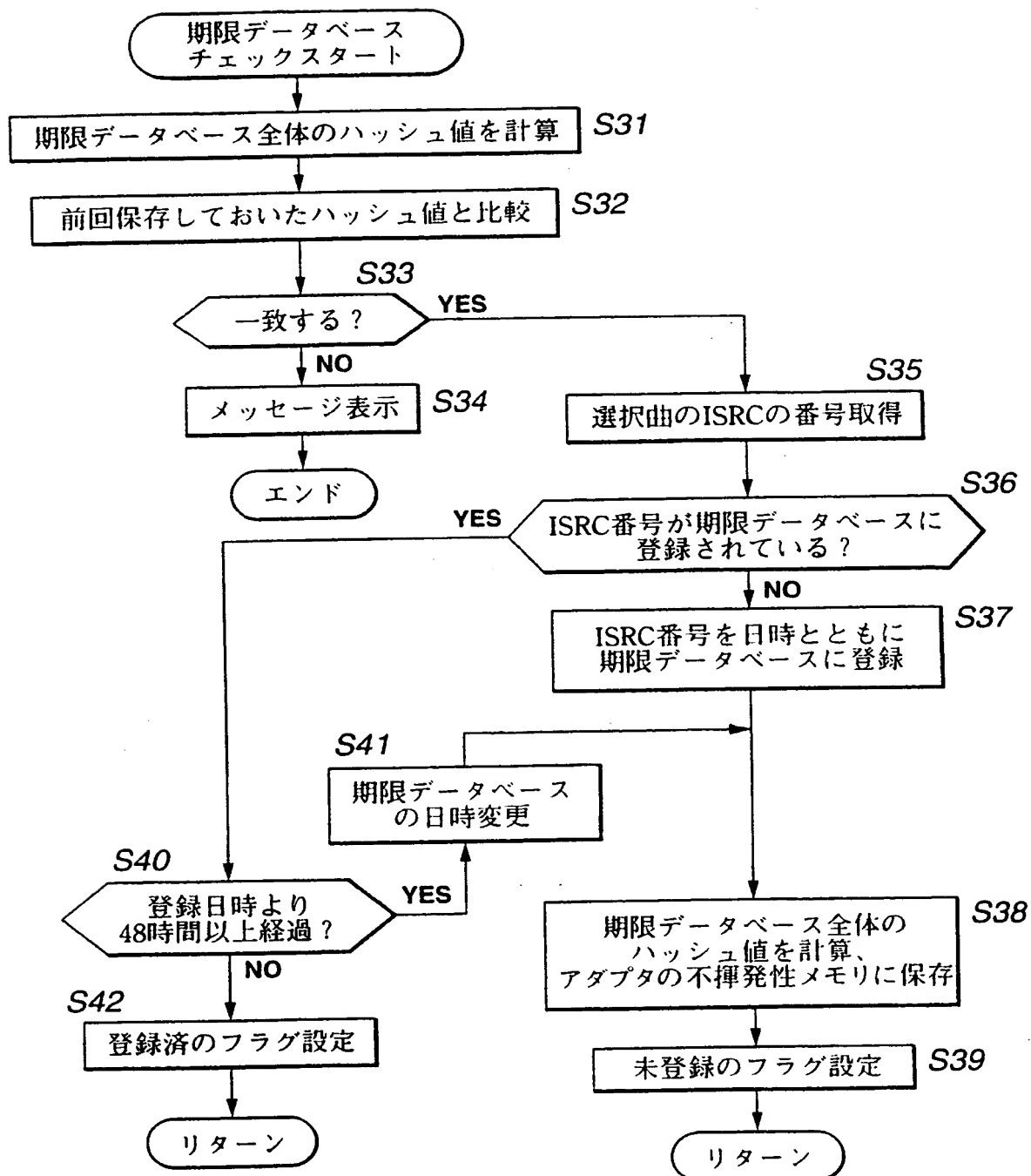


FIG.8

9/36

期限データベース

	アイテム 1	アイテム 2	アイテム 3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16:15	

ハッシュ値	0xf3352e125934
-------	----------------

FIG.9

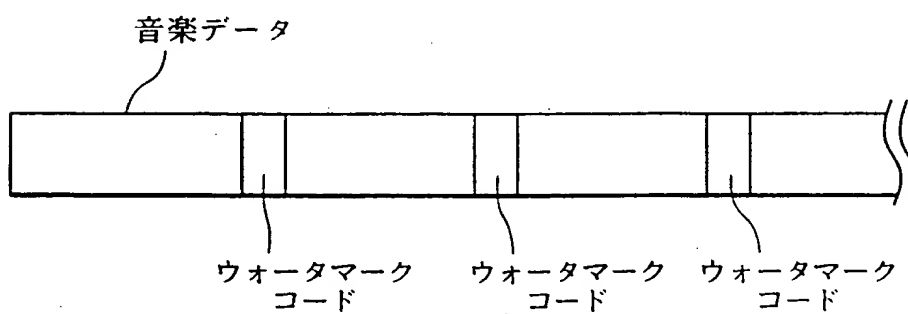


FIG.10

10/36

曲データベース

	アイテム 1	アイテム 2	アイテム 3
ファイル名	Xd000110. st2	px92341234. at2	aa0234287034. at2
暗号化された暗号鍵	0xabababababab	0x9898989898989	0x123456789012
曲名	春の小川	運命	荒城の月
長さ	180	190	200
再生条件 : 開始日時	-	2001.01.01.00:00	-
再生条件 : 終了日時	1999.07.31.23:59	-	-
再生条件 : 回数制限	-	20	-
再生回数カウンタ	-	12	-
再生時課金条件	-	-	¥5
コピー条件 : 回数	2	0	0
コピー回数カウンタ	1	0	0
コピー条件 : SCMS	0b01	0b10	0b00

ハッシュ値 0xf9951e566321

FIG.11

11/36

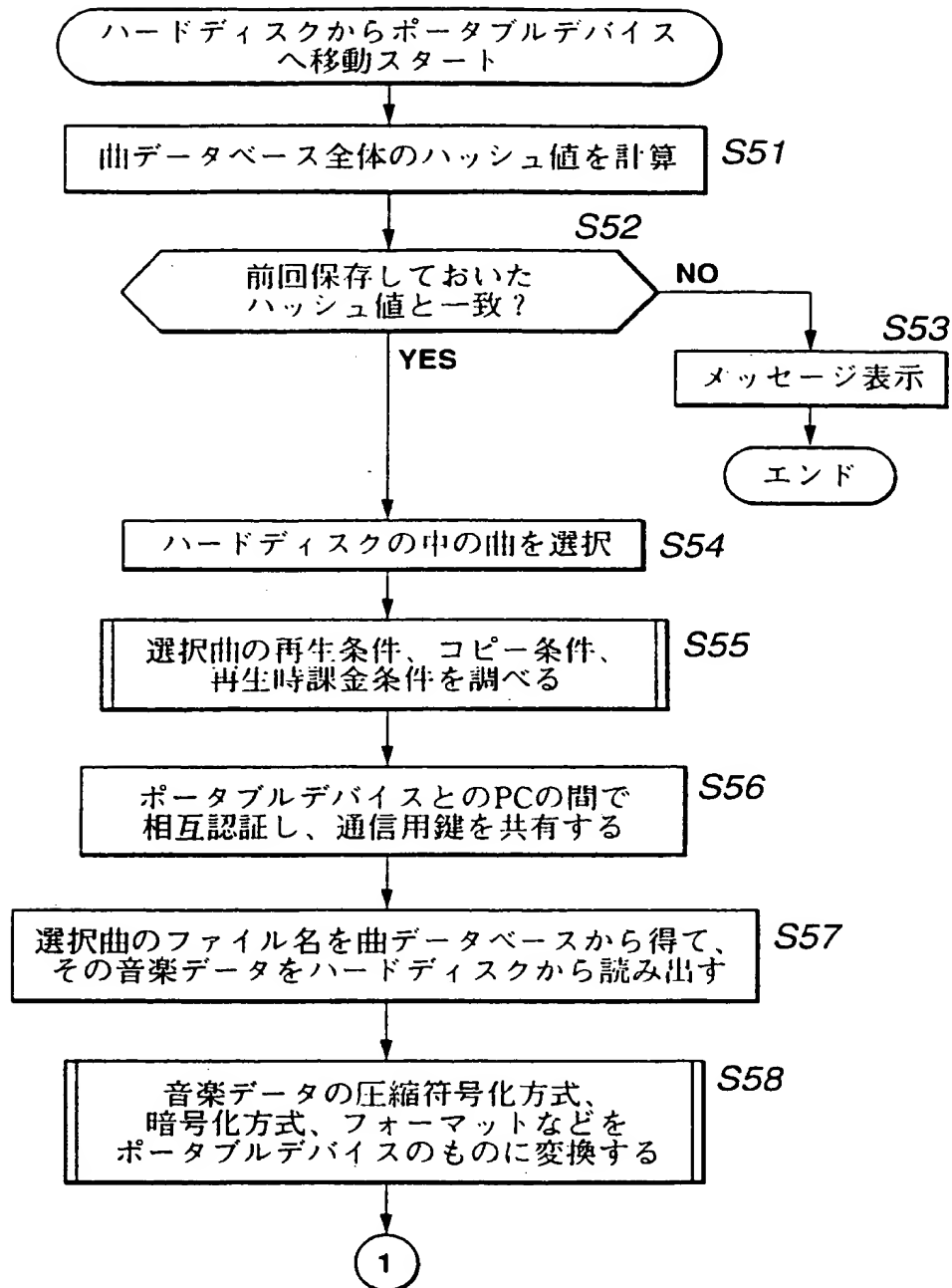


FIG.12A

12/36

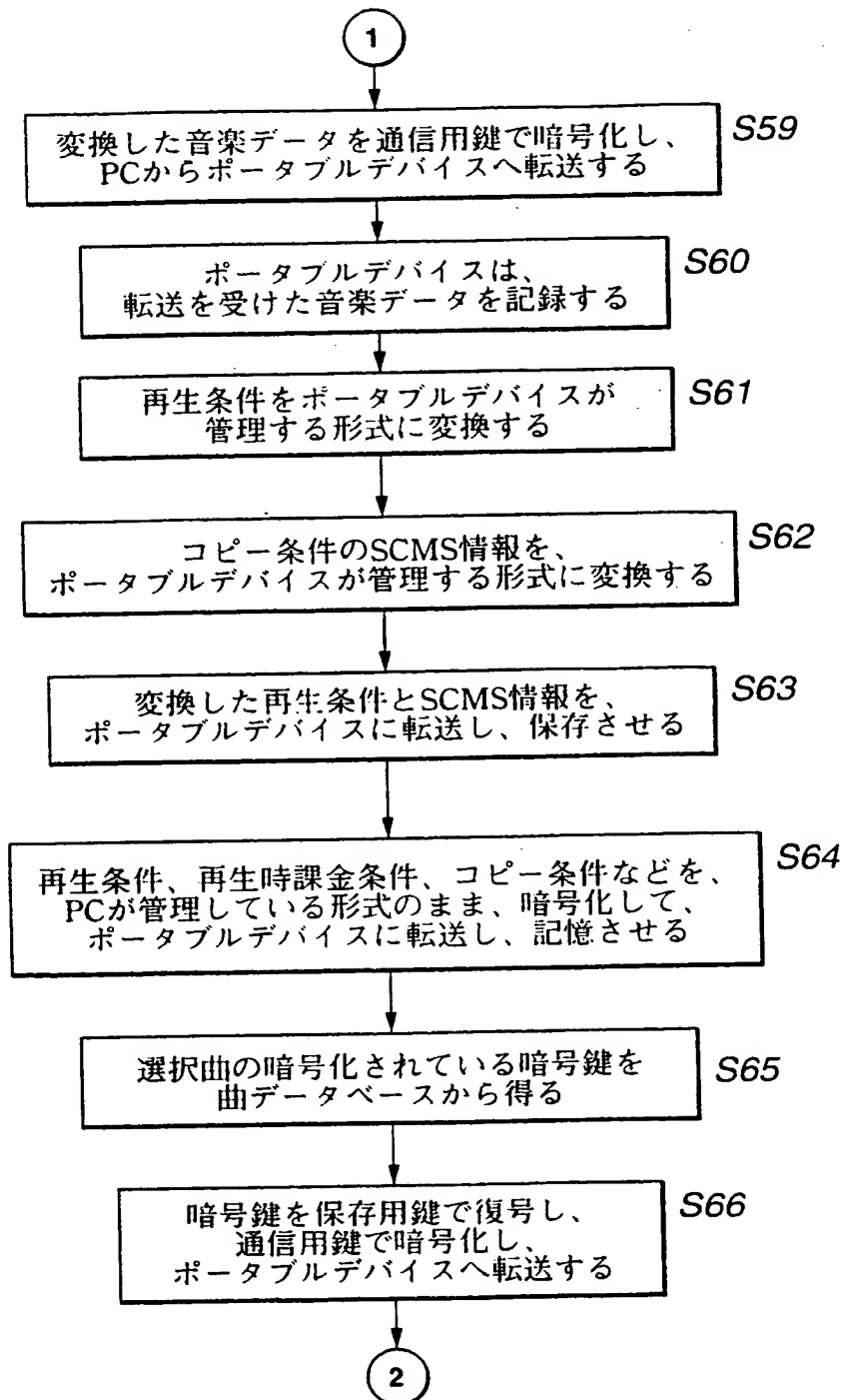


FIG.12B

13/36

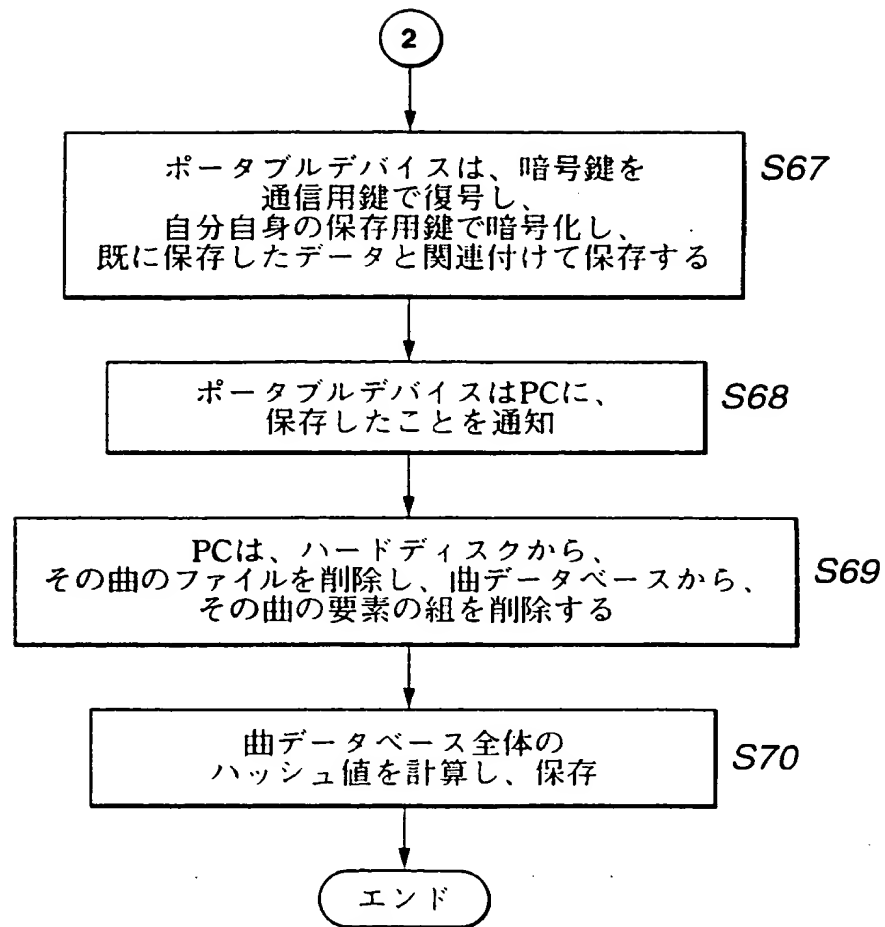


FIG.12C

14/36

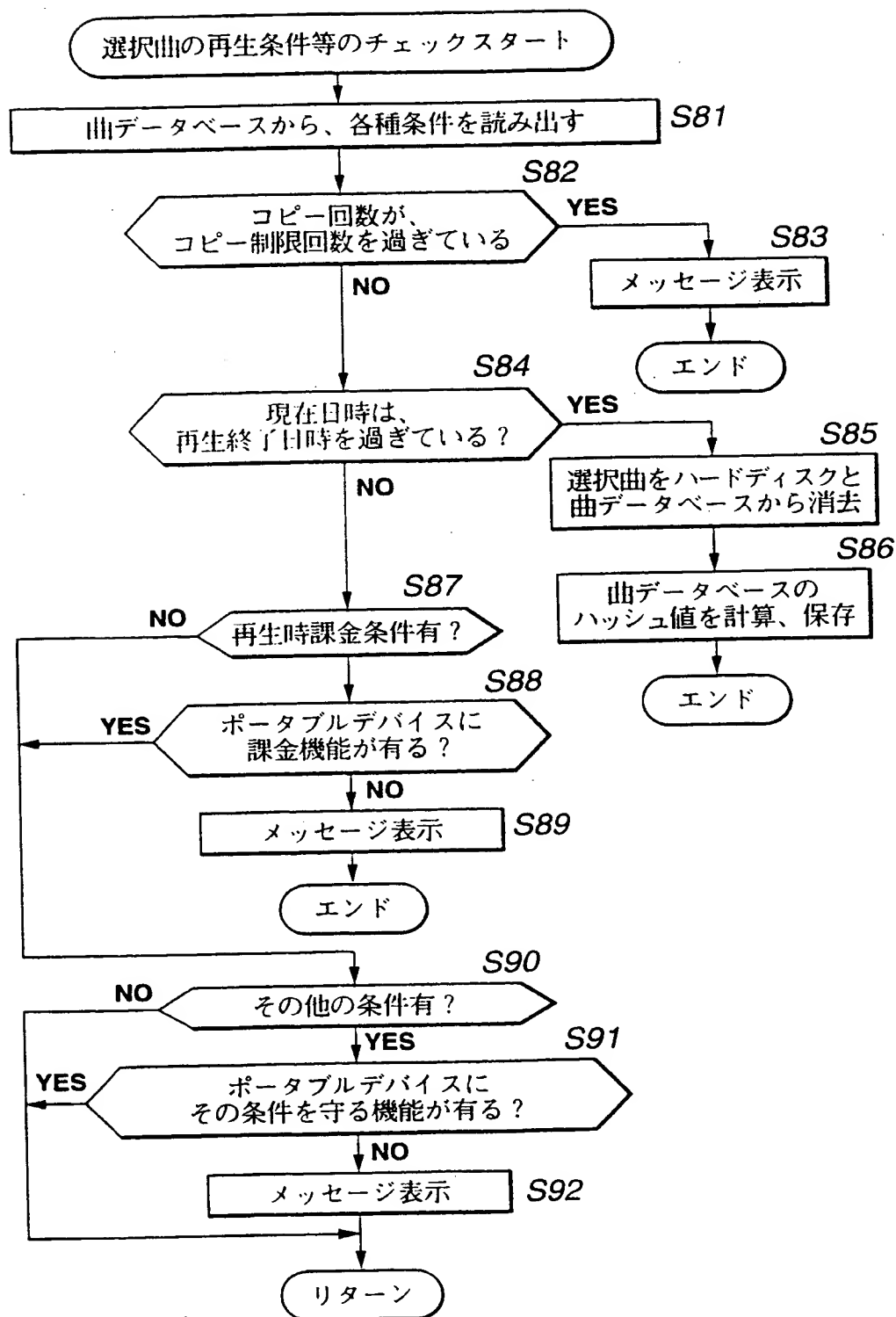


FIG.13

15/36

ポータブルデバイスが管理している再生条件

	アイテム 1	アイテム 2	アイテム 3
曲 ID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

FIG.14

16/36

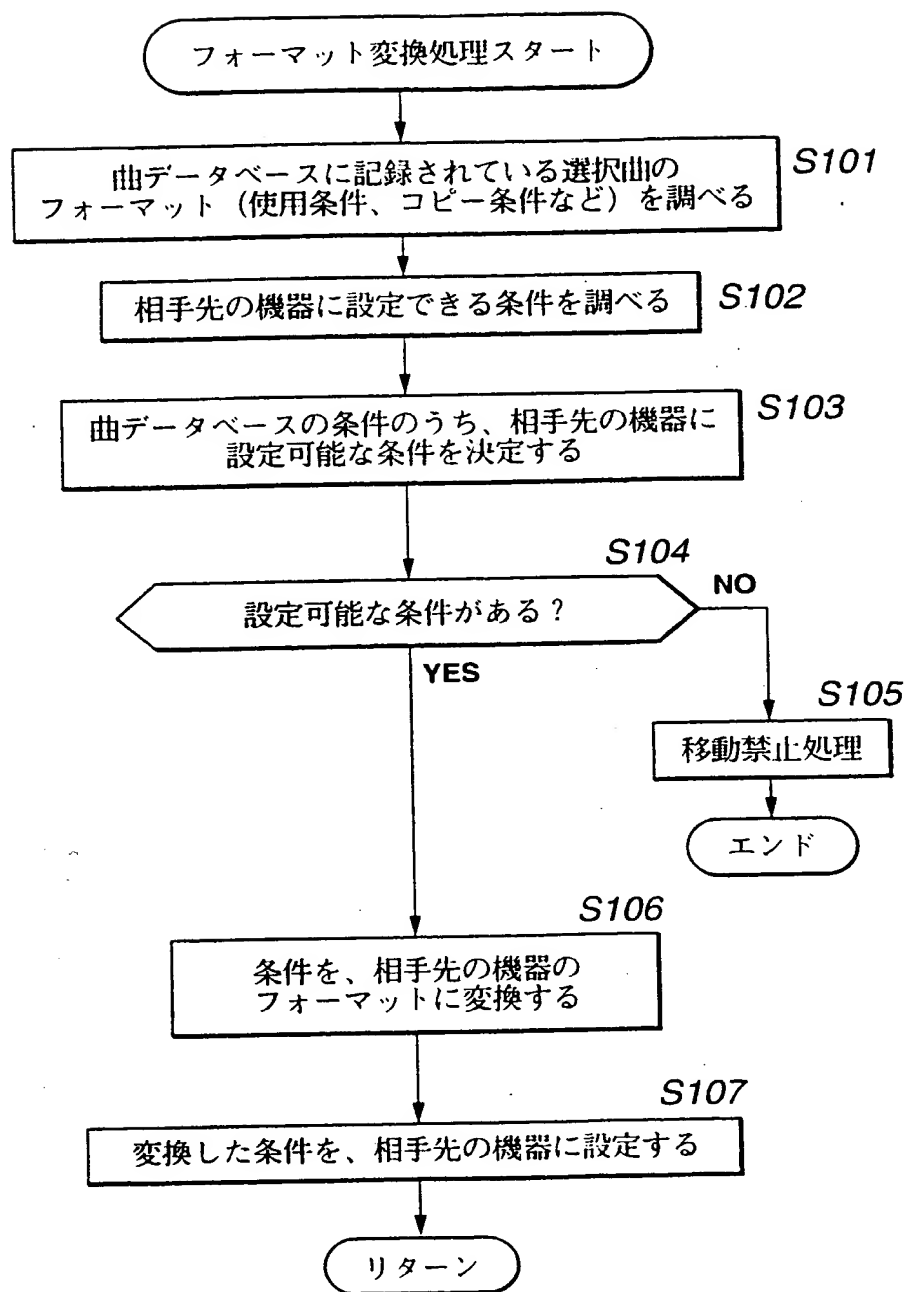


FIG.15

17/36

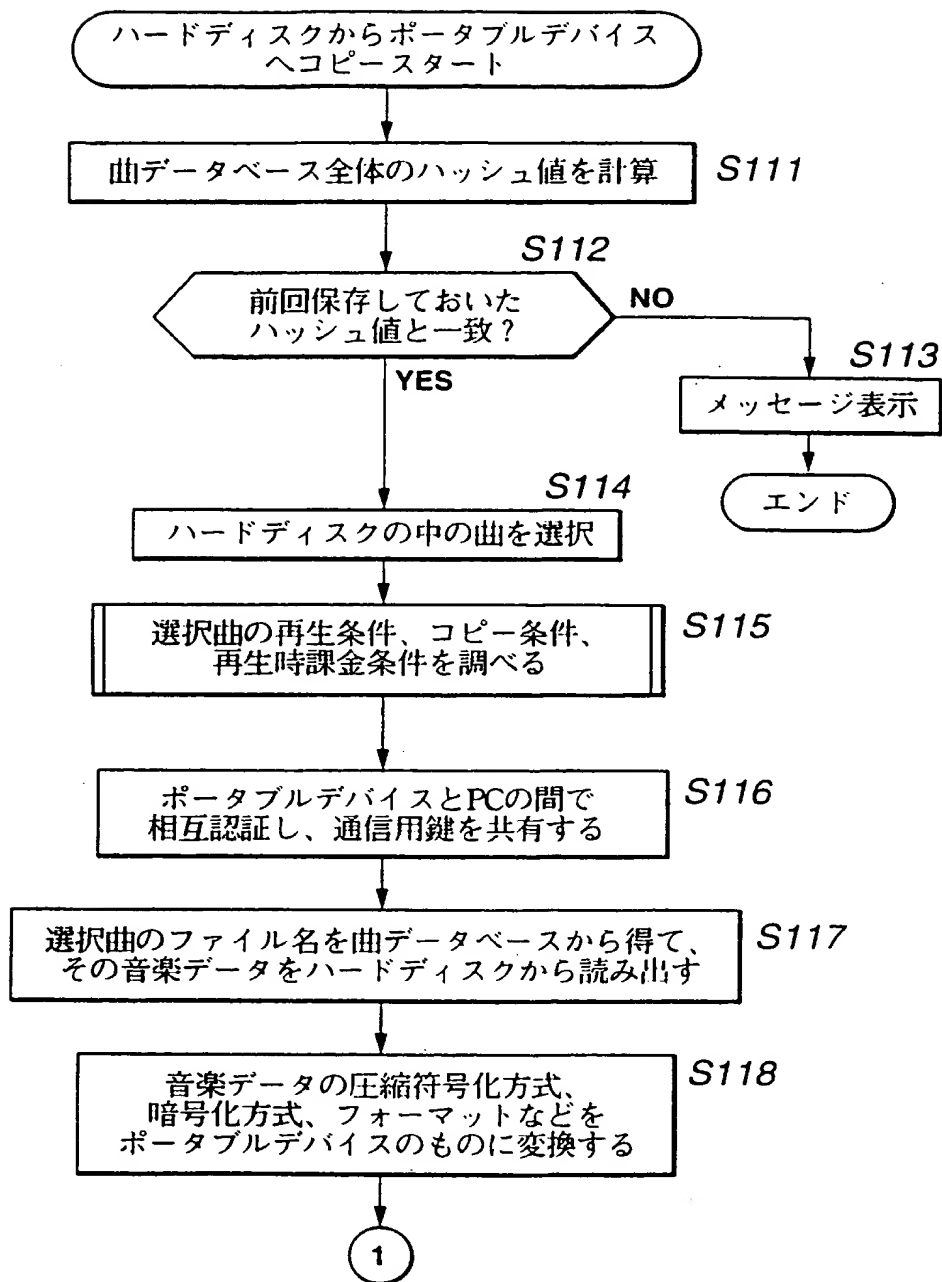


FIG.16A

18/36

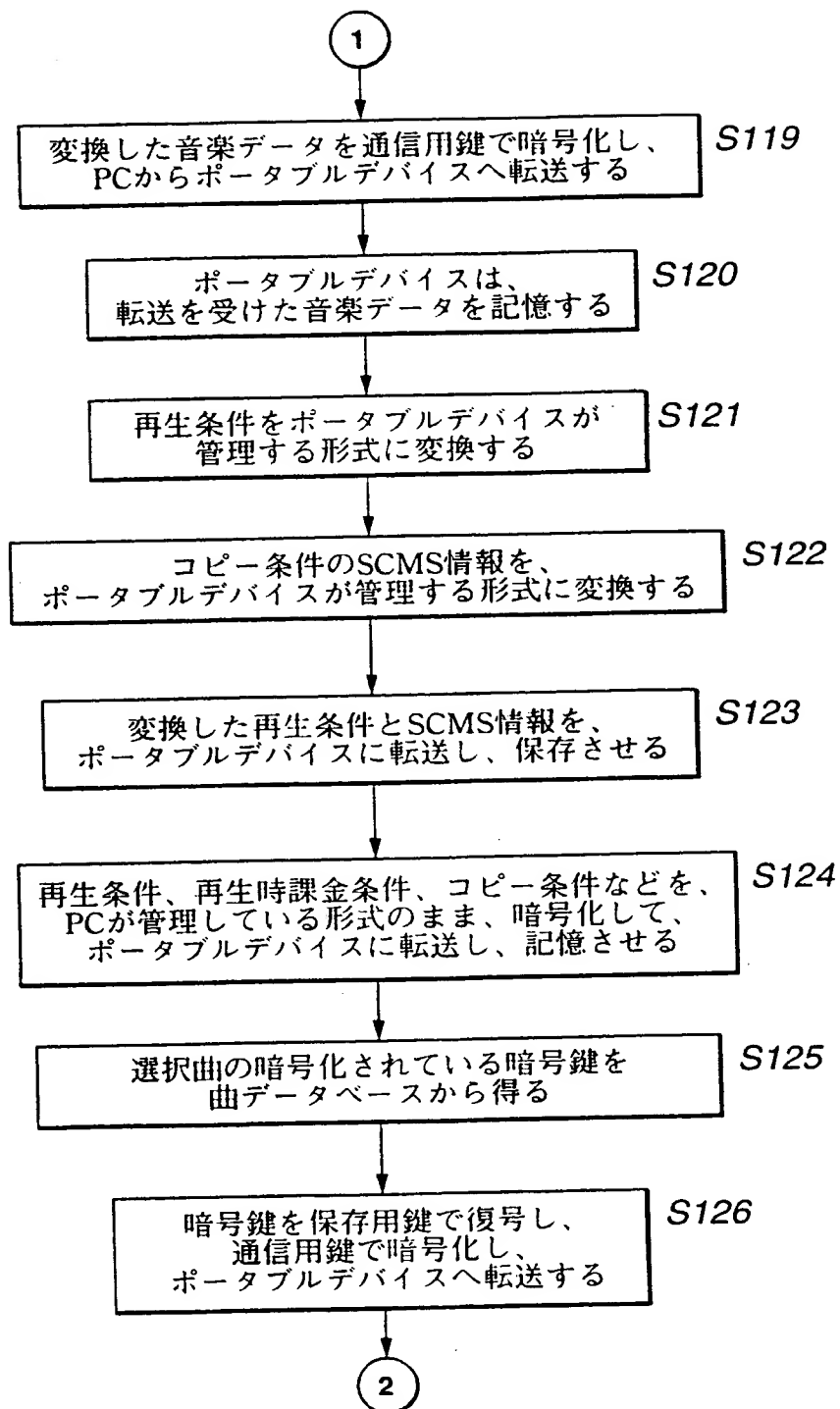


FIG.16B

19/36

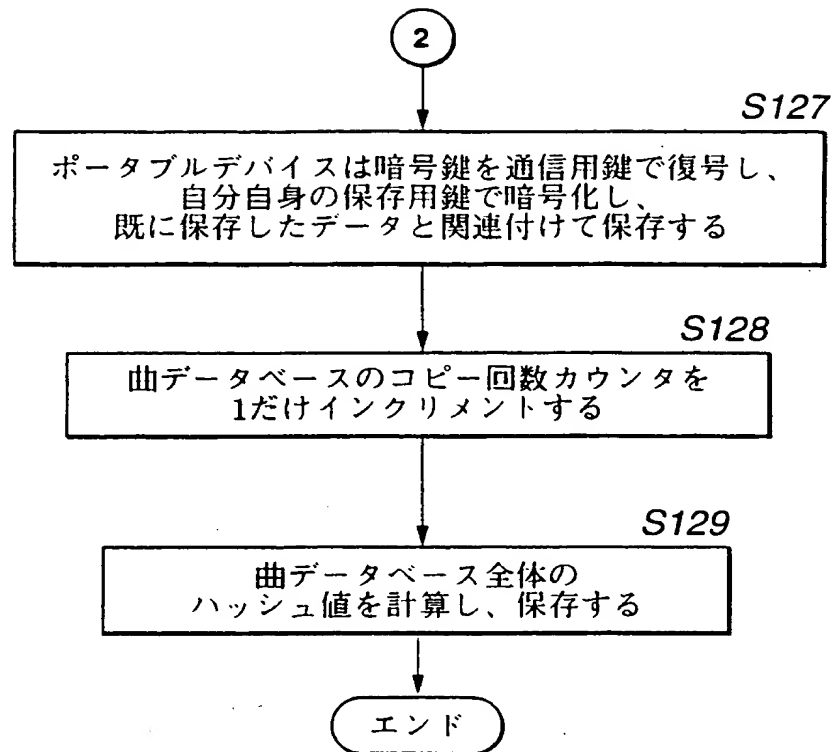


FIG.16C

20/36

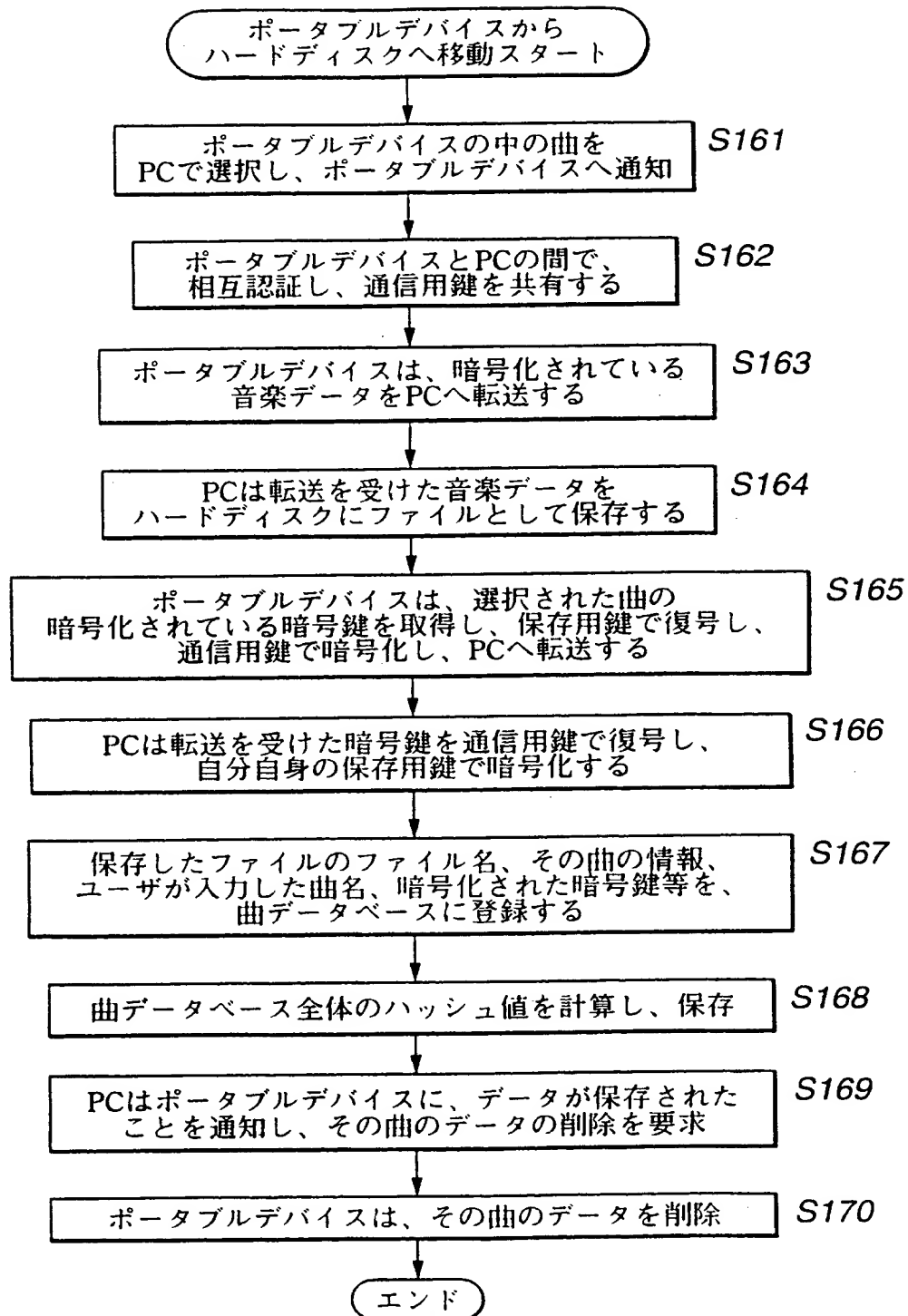


FIG.17

23/36

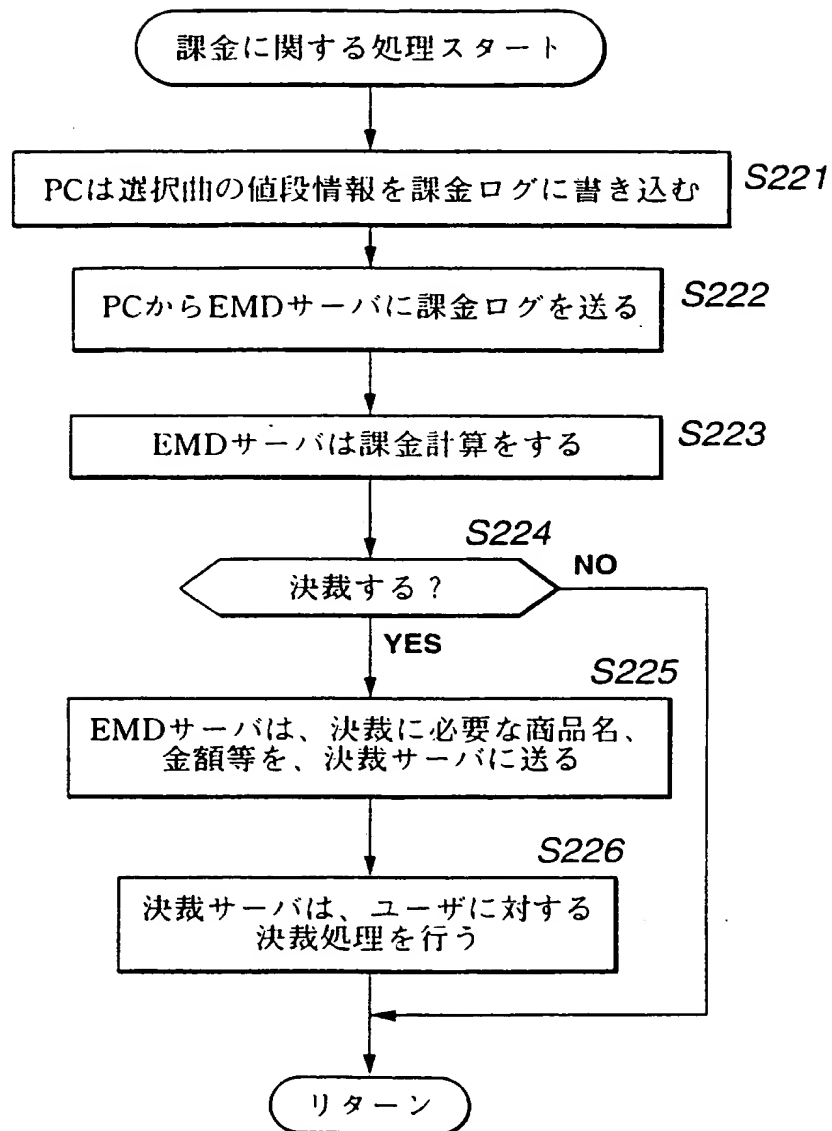


FIG.20

24/36

課金ログ

	アイテム 1	アイテム 2	アイテム 3	
料金	50	50	50	

ハッシュ値	0xf8783e263517
-------	----------------

FIG.21

21/36

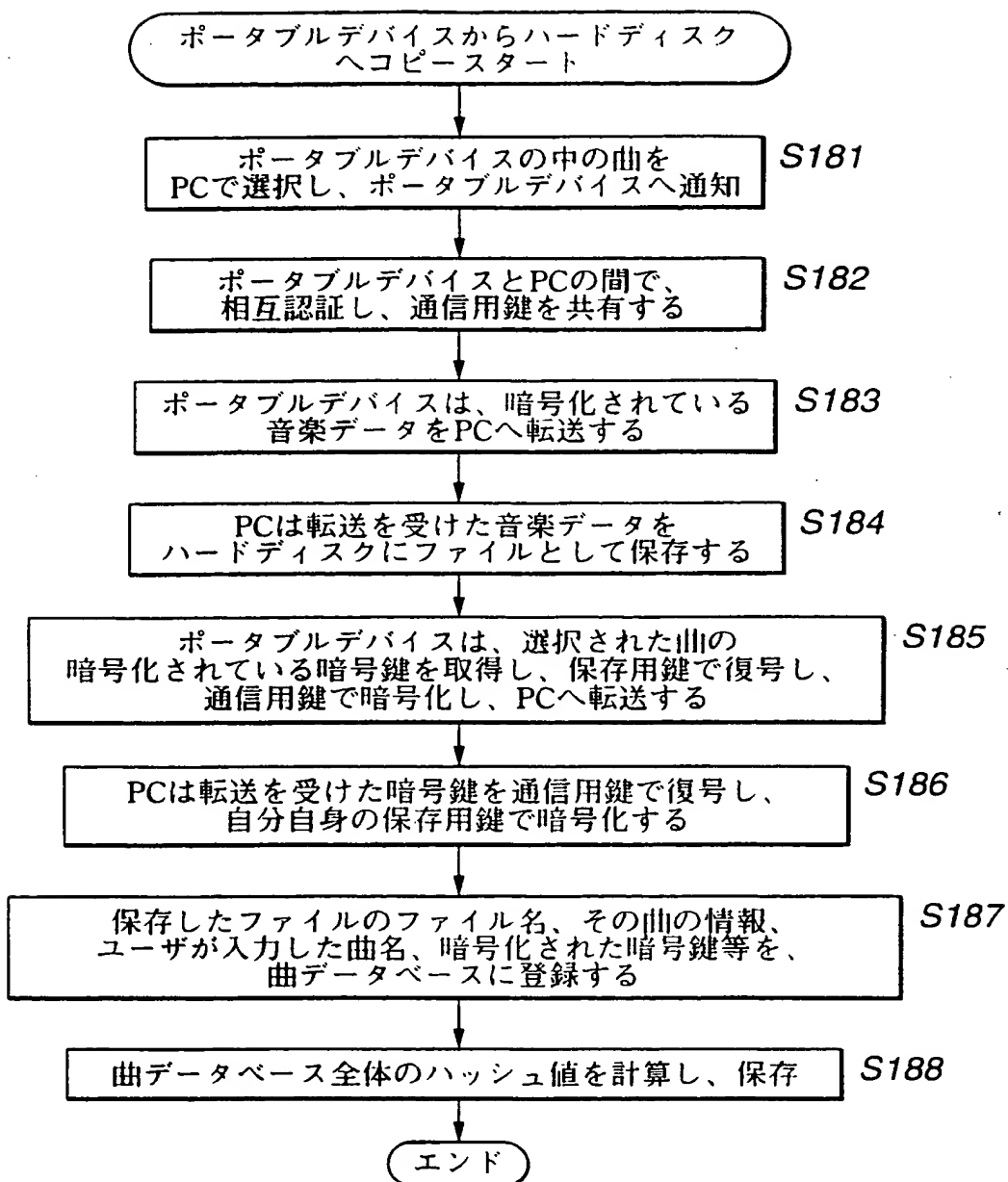


FIG.18

22/36

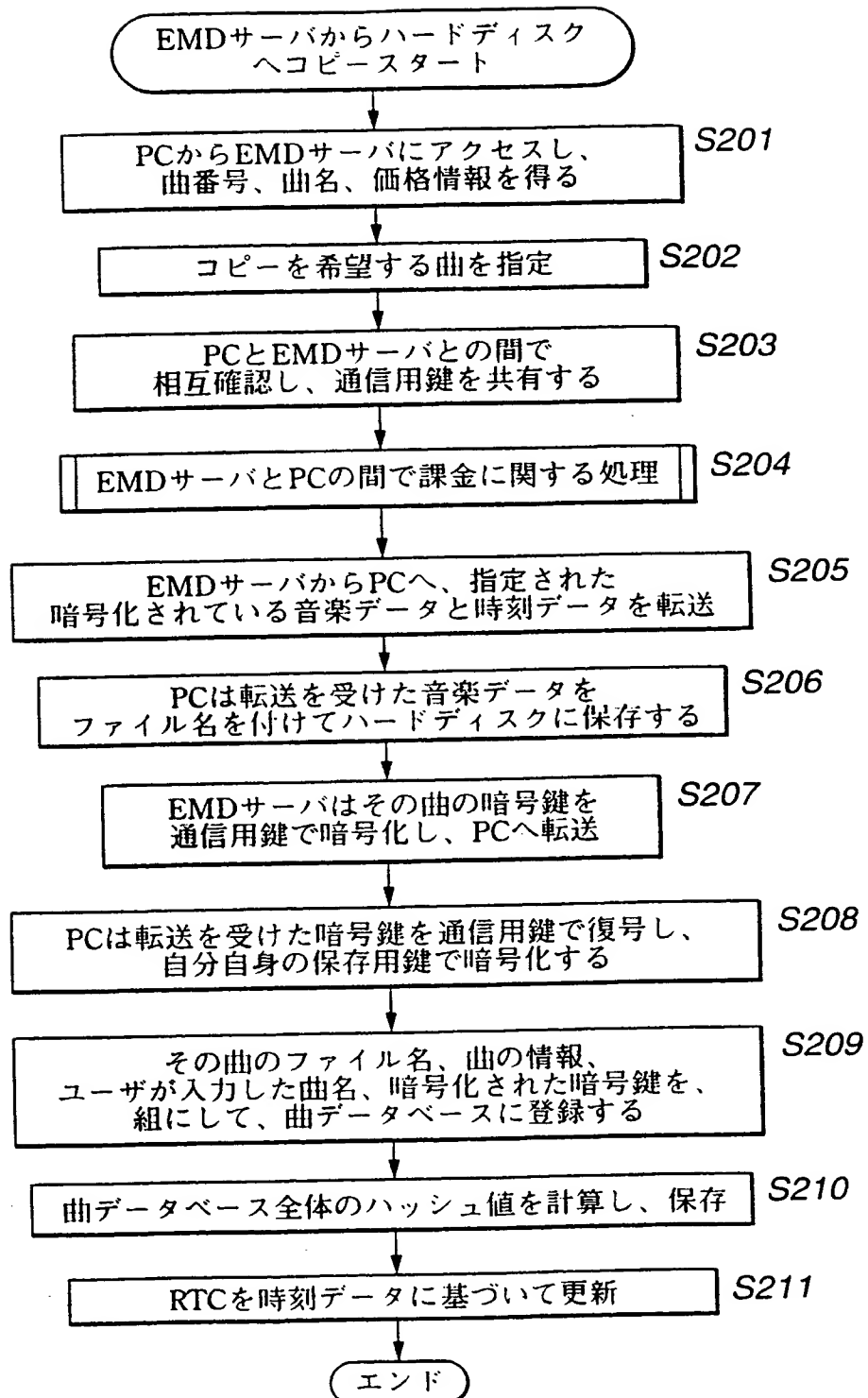


FIG.19

25/36

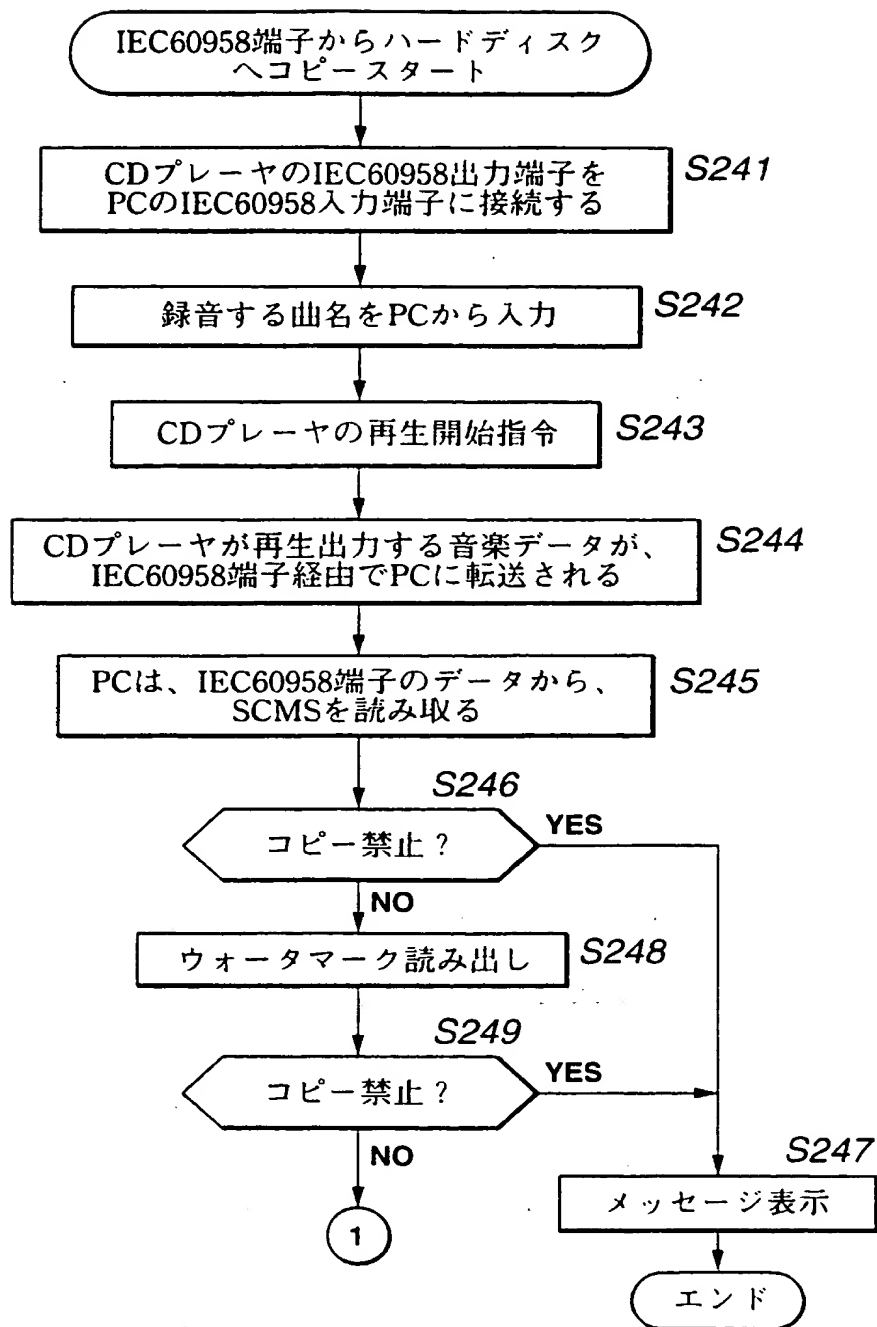


FIG.22A

26/36

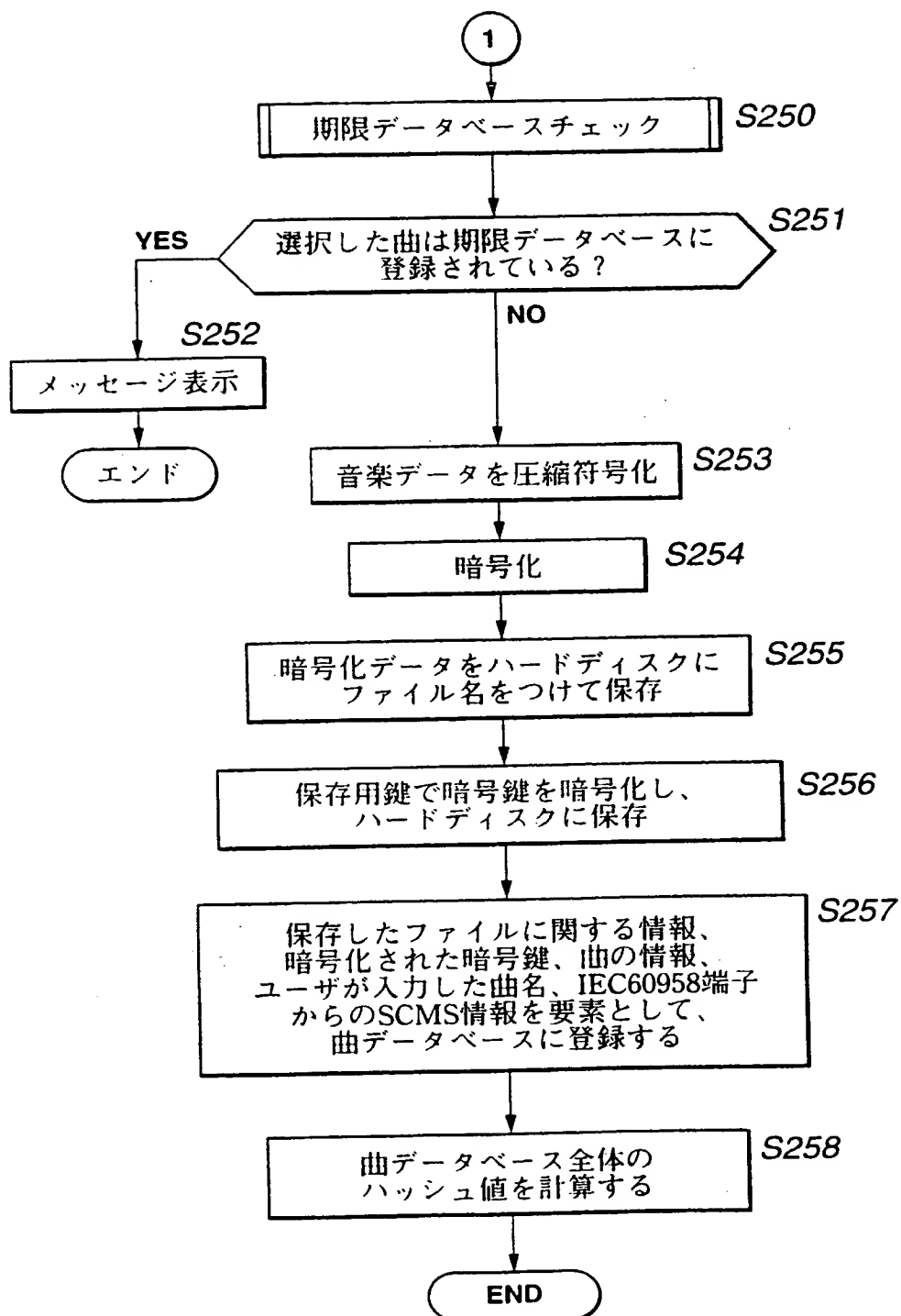


FIG.22B

27/36

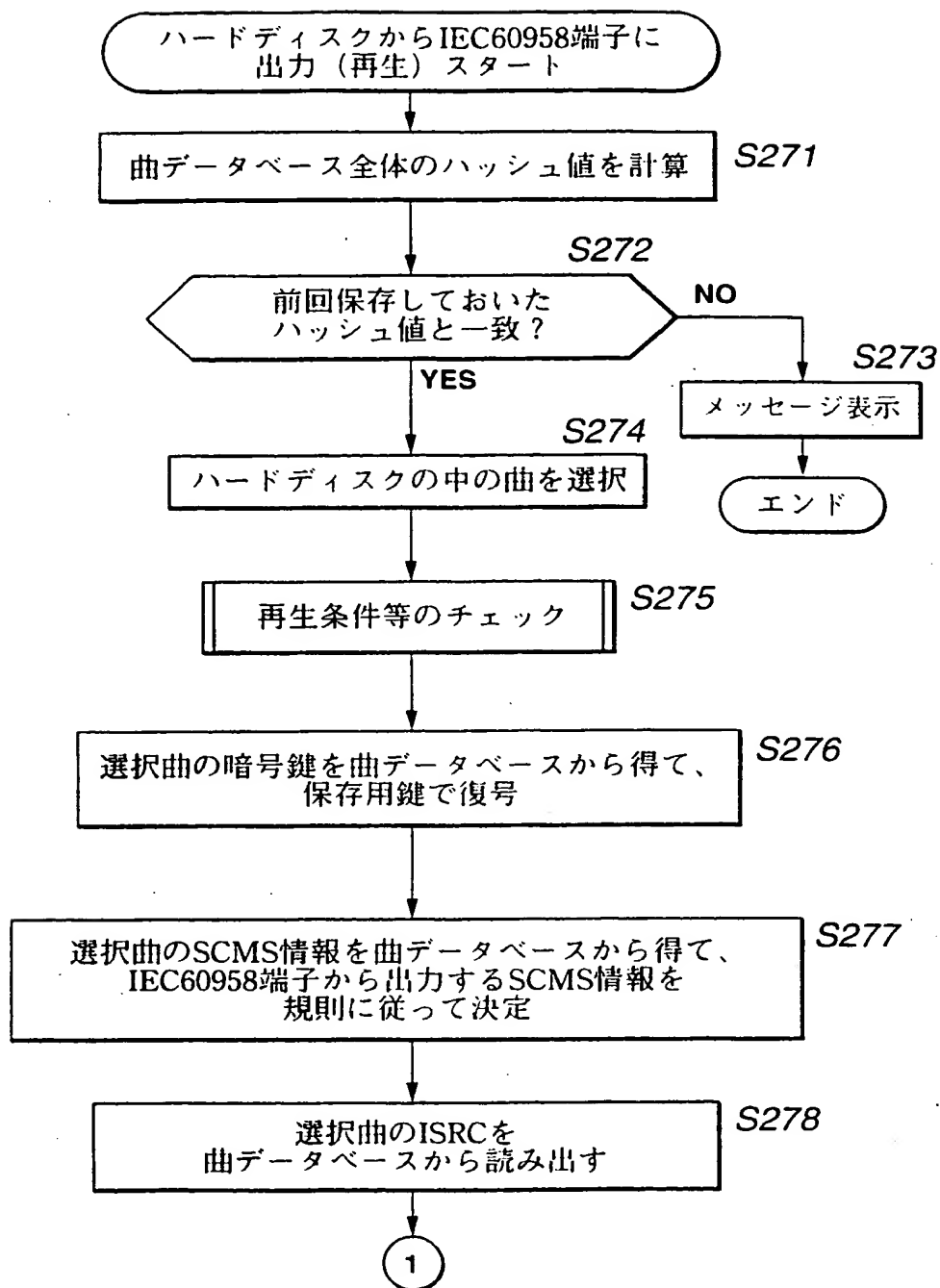


FIG.23A

28/36

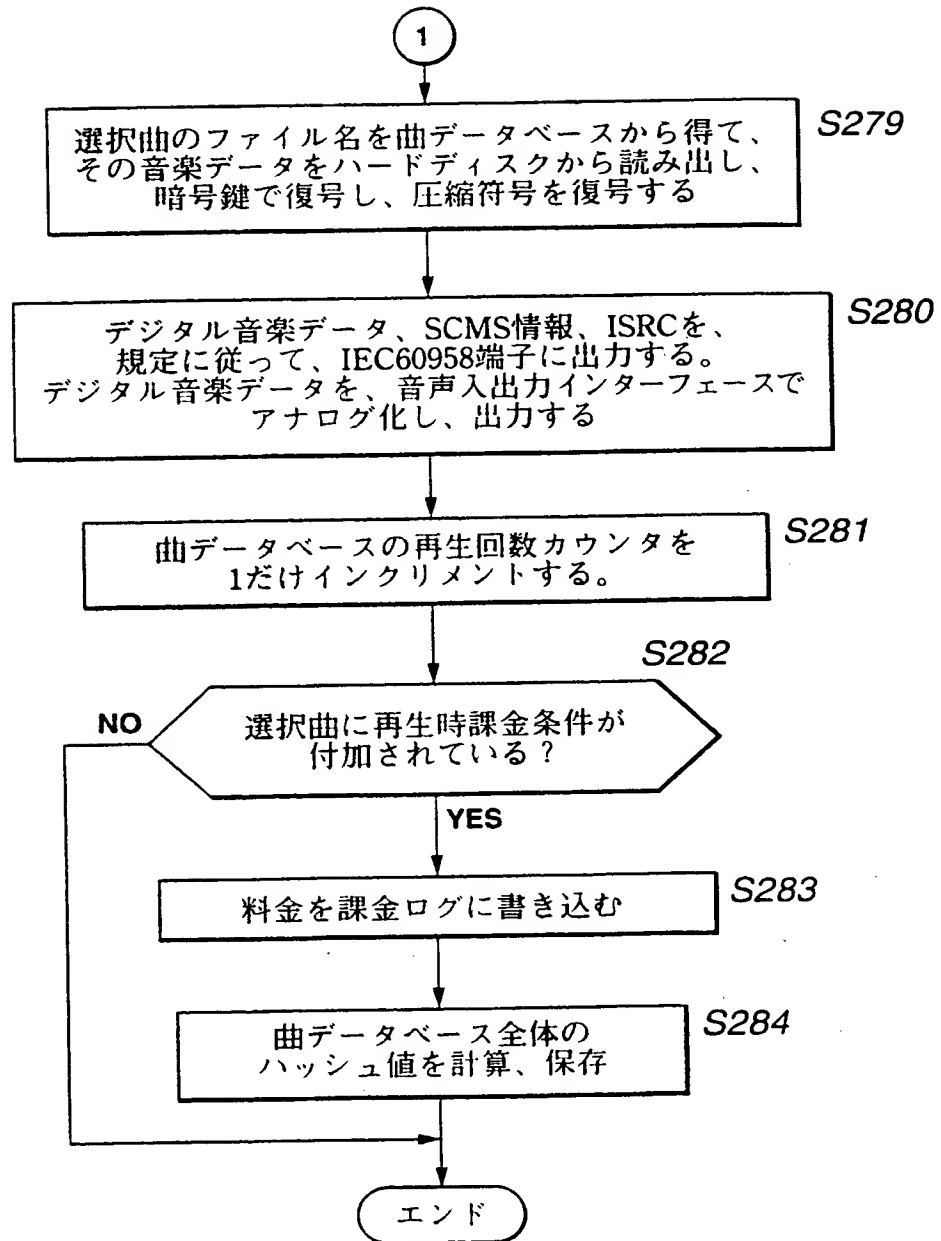


FIG.23B

29/36

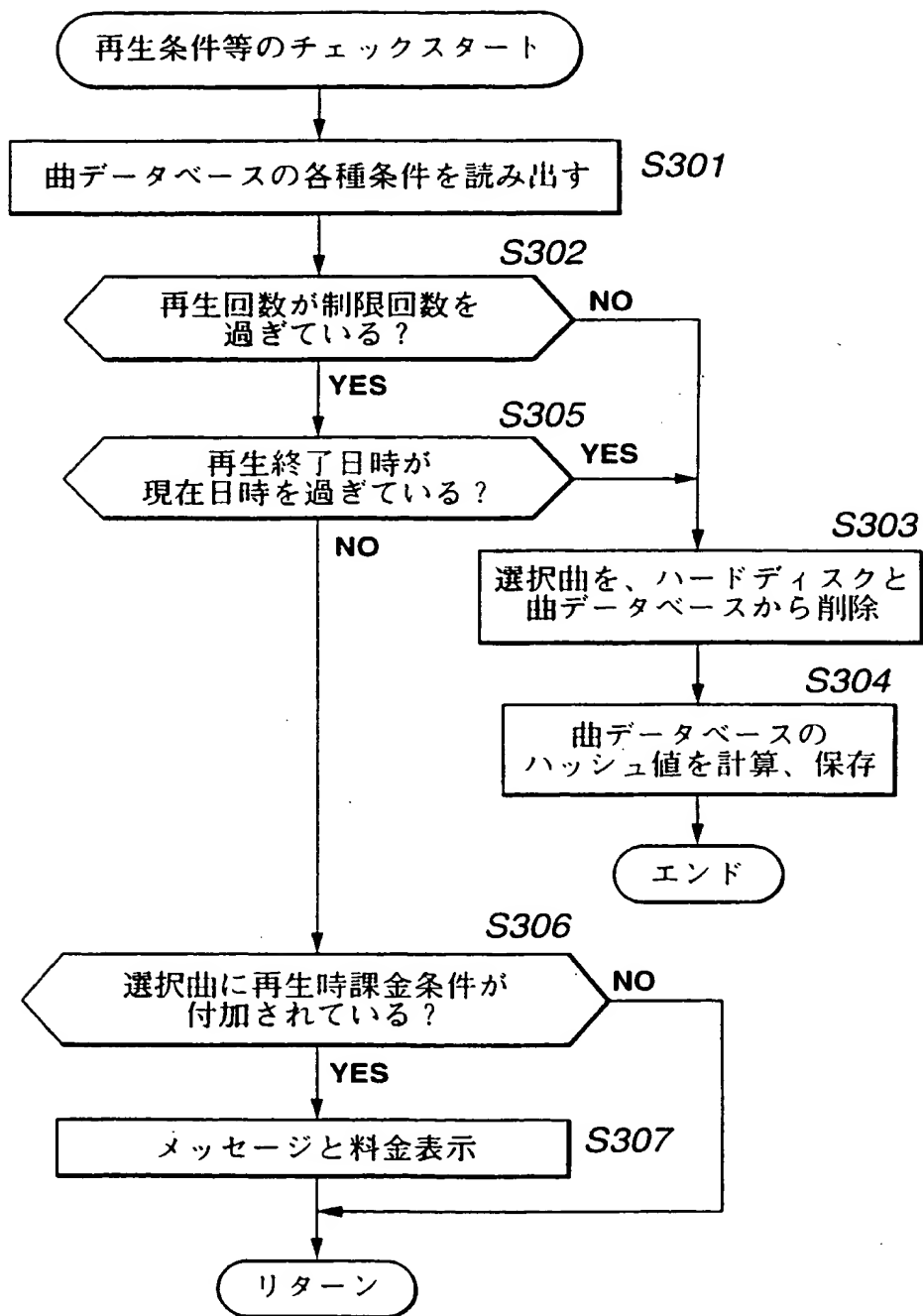


FIG.24

30/36

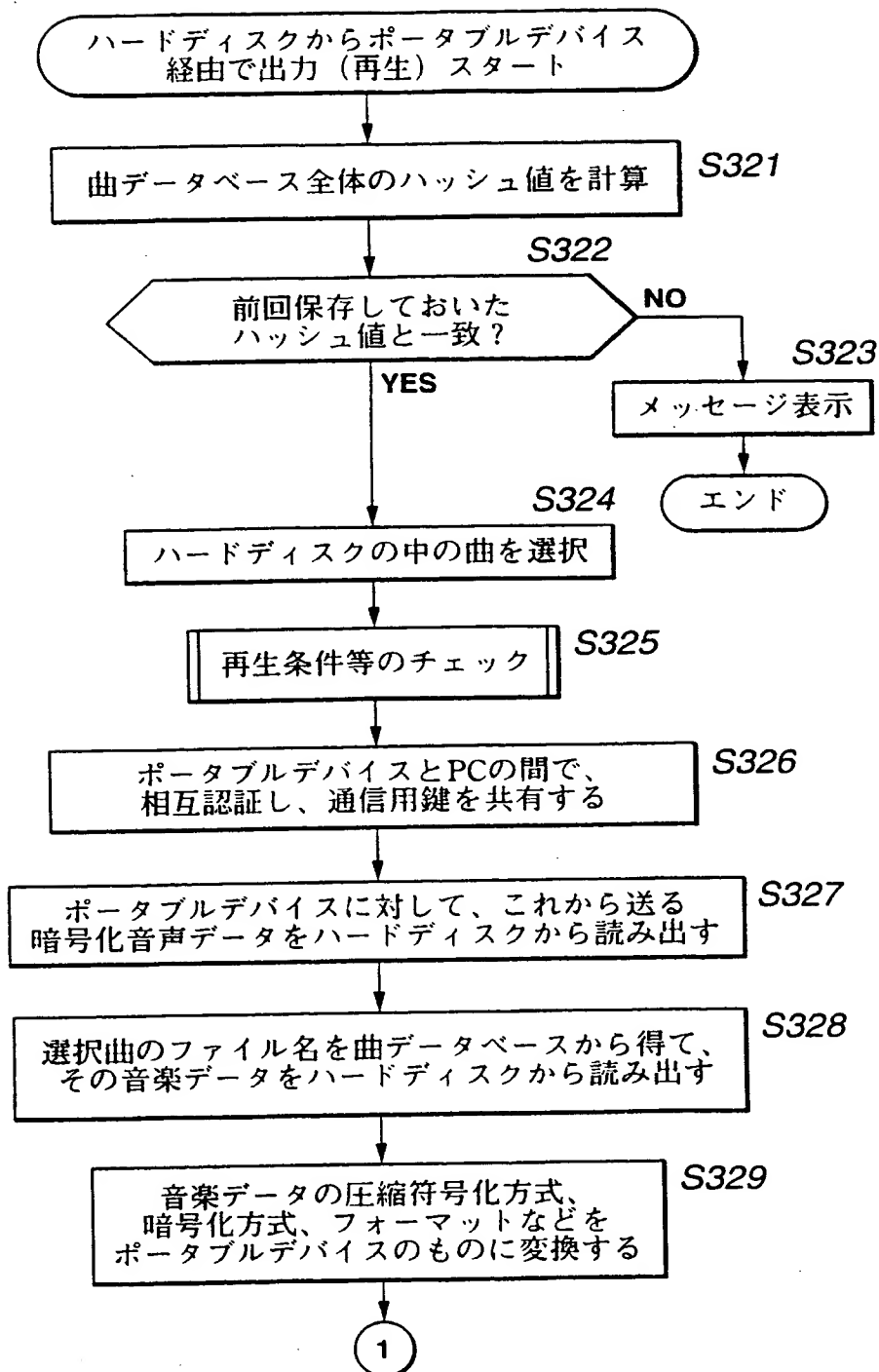


FIG.25A

31/36

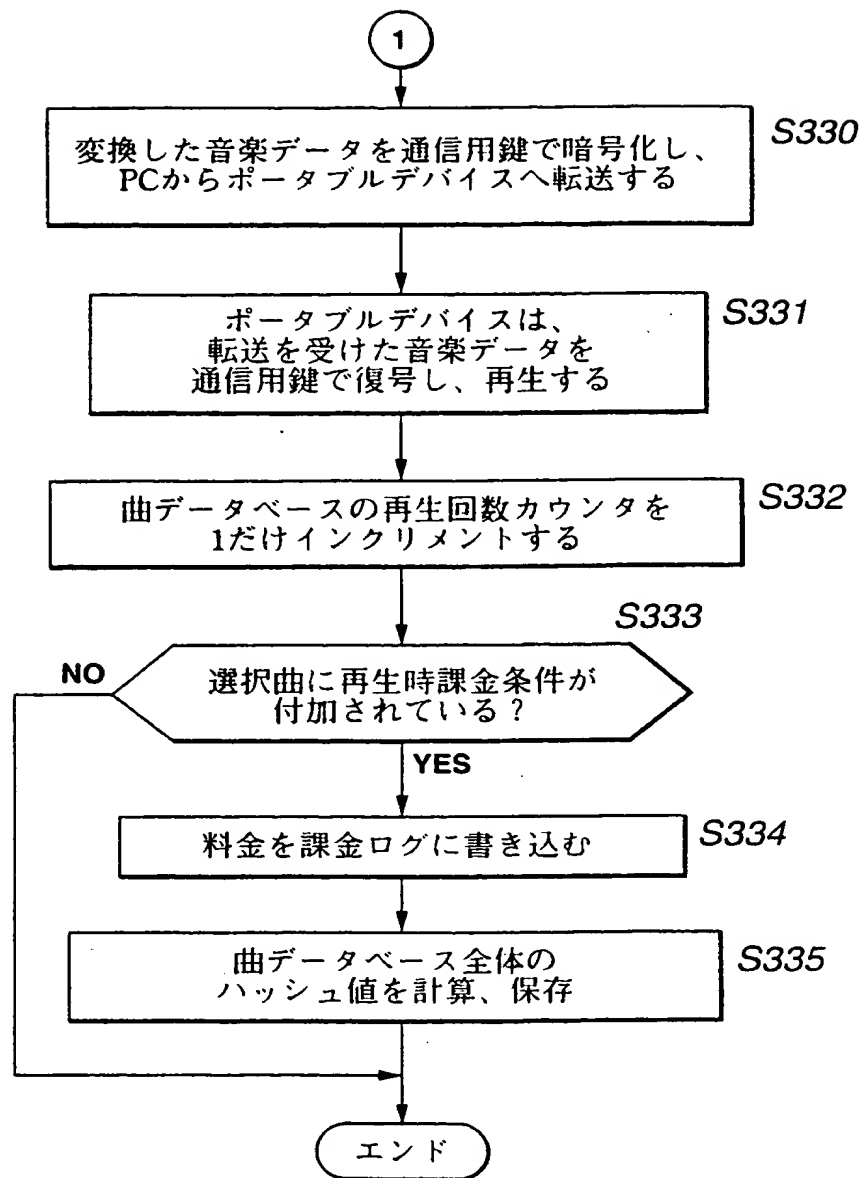


FIG.25B

32/36

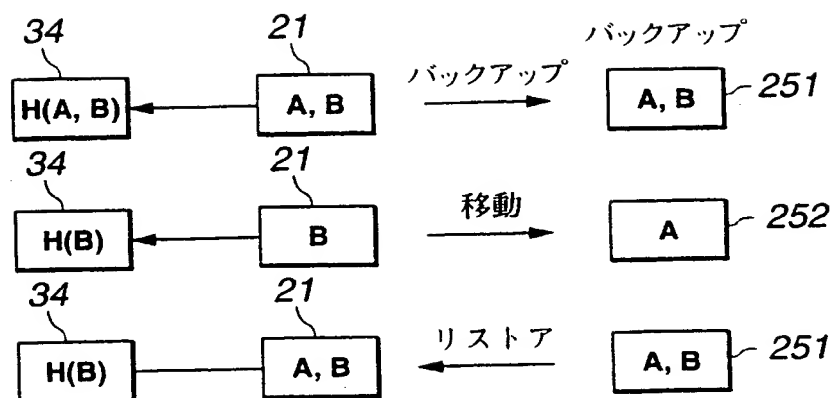


FIG.26

33/36

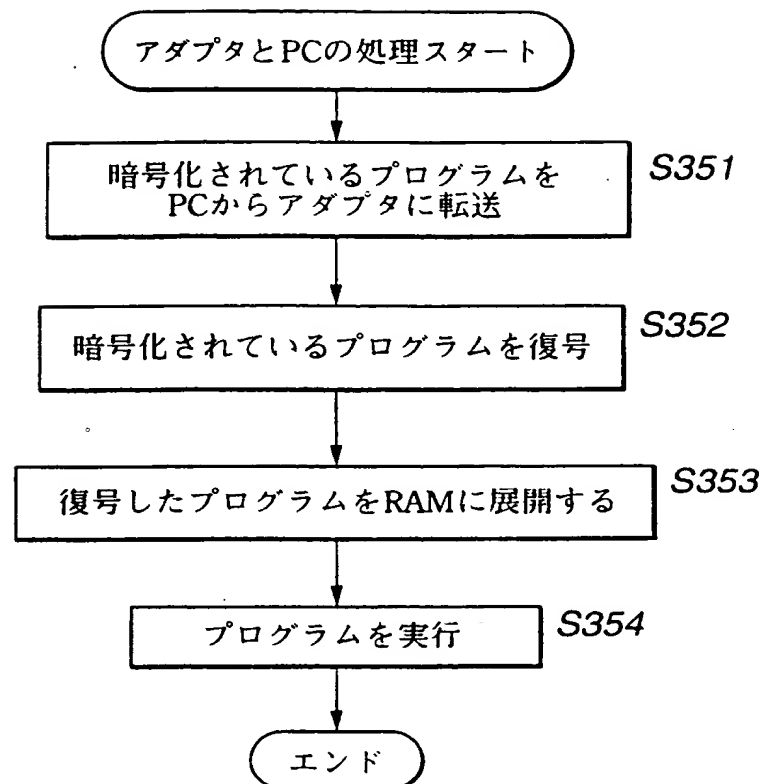


FIG.27

34/36

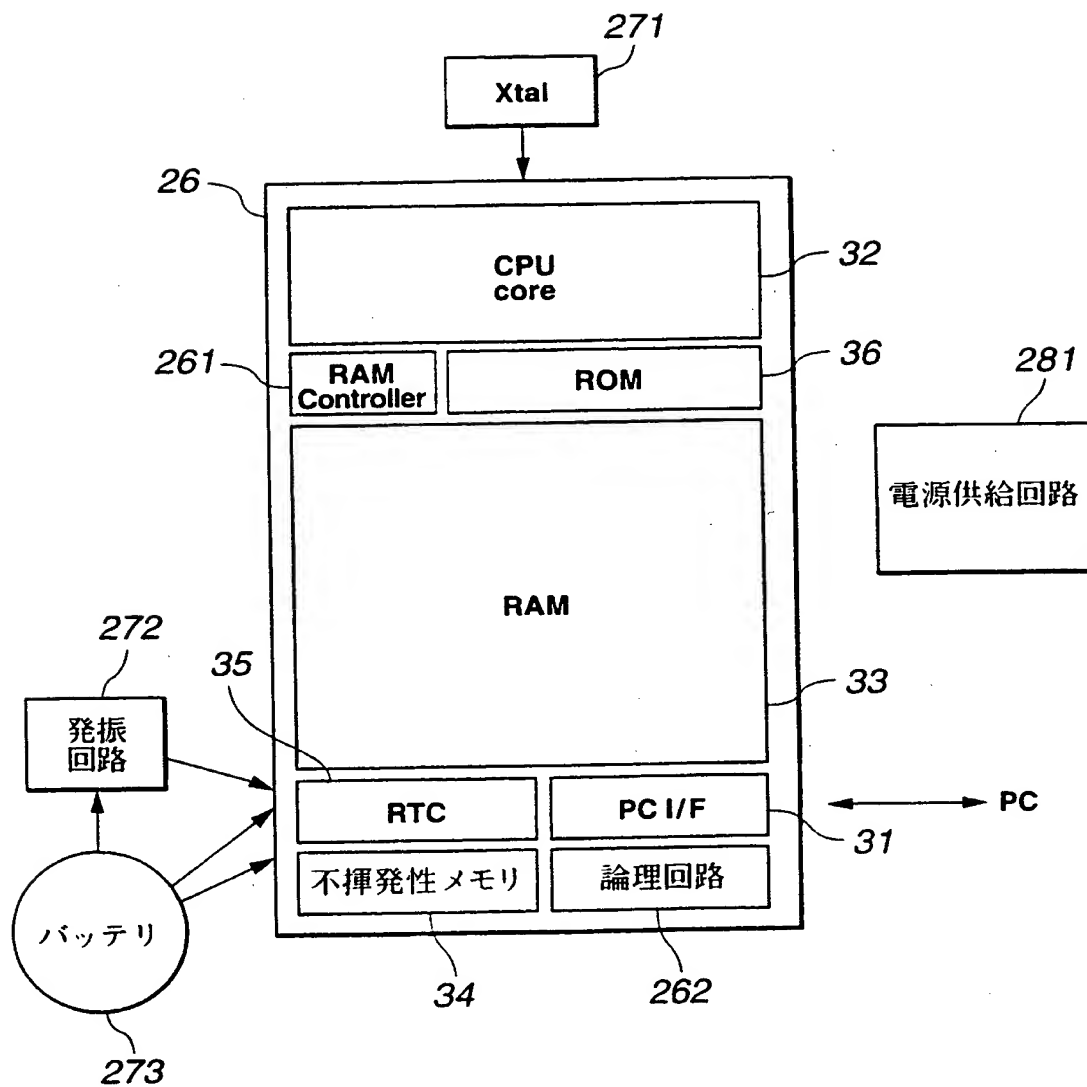


FIG.28

FIG.29A

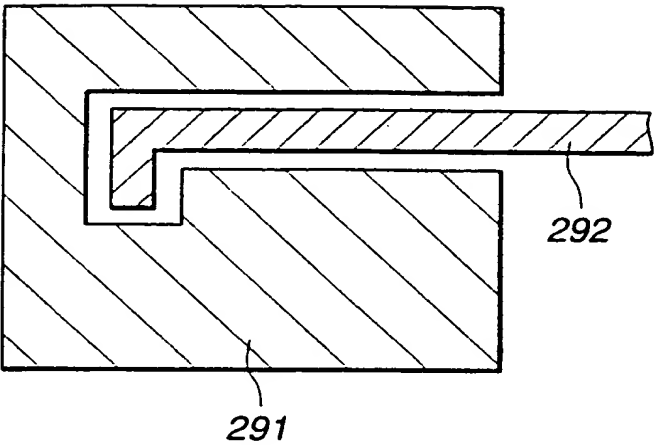
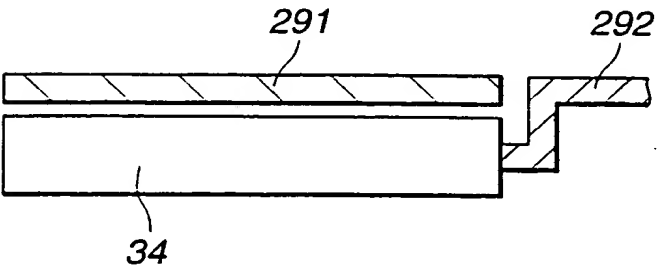


FIG.29B



36/36

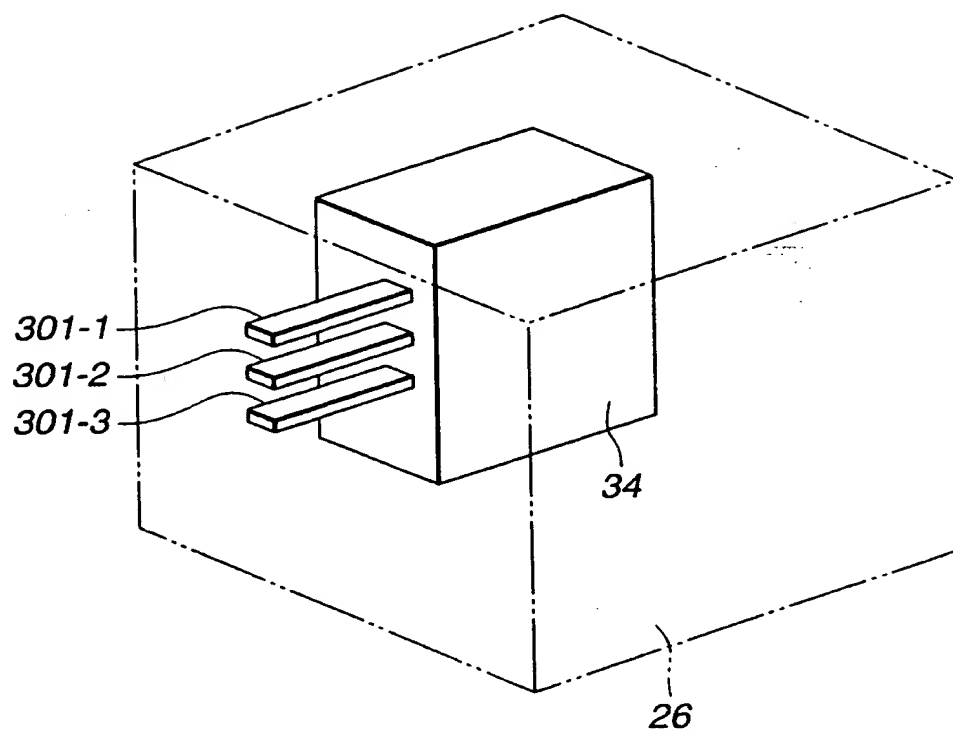


FIG.30

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/07302

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G11B20/10, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G11B20/10, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2000
Kokai Jitsuyo Shinan Koho	1971-2000	Jitsuyo Shinan Toroku Koho	1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 3-250878, A (Canon Inc.), 08 November, 1991 (08.11.91), Full text; Figs. 1 to 8 (Family: none)	1-3
A	JP, 8-195064, A (Sony Corporation), 30 July, 1996 (30.07.96), Full text; Figs. 1 to 8 & AU, 4058995, A & EP, 718840, A & US, 5923486, A	1-3

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
24 March, 2000 (24.03.00)

Date of mailing of the international search report
04 April, 2000 (04.04.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁷ G11B20/10, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl⁷ G11B20/10, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2000年
日本国登録実用新案公報 1994-2000年
日本国実用新案登録公報 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 3-250878, A (キャノン株式会社) 8. 11. 1991 (08. 11. 91) 全文, 第1-8図 (ファミリーなし)	1-3
A	J P, 8-195064, A (ソニー株式会社) 30. 7月. 1996 (30. 07. 96) 全文, 第1-8図 & AU, 4058995, A & EP, 718840, A & US, 5923486, A	1-3

☐ C欄の続きにも文献が列举されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

24. 03. 00

国際調査報告の発送日

(04.04.00)

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

小松 正

印

5Q

7736

電話番号 03-3581-1101 内線 6922

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)